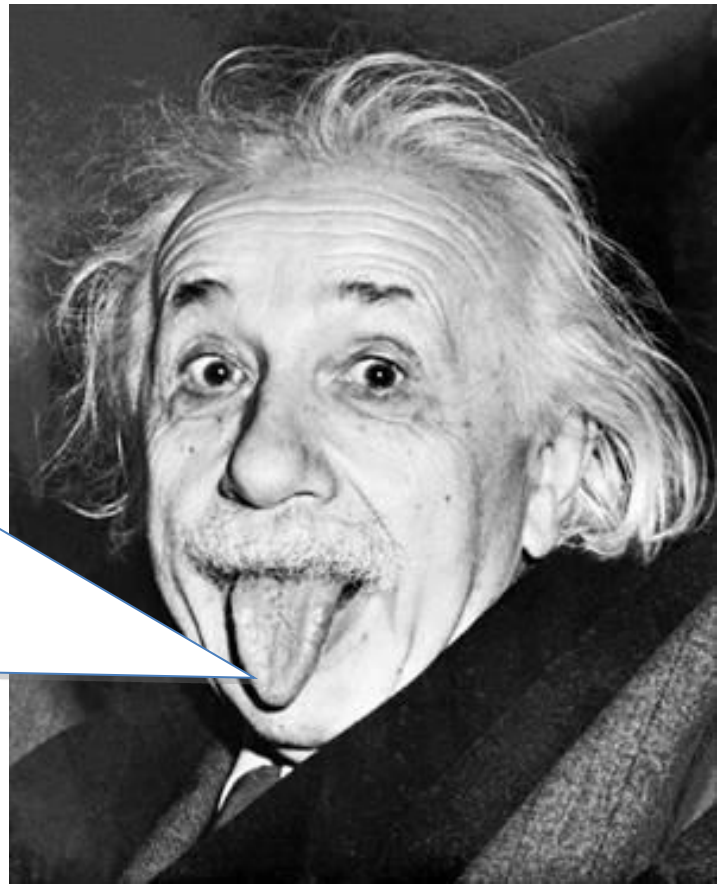
Taste the power of Crimeware!

(HIT 2010 Edition)



Anthony Lai

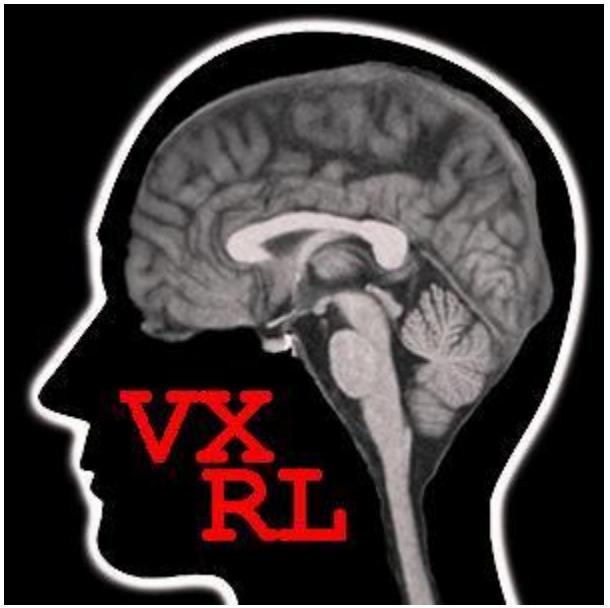
Security Researcher@VXRL

Special Thanks

- HIT fellows
- Thank you to PK and Birdman
- My wife and Pomeranian family

My Bio

- From Hong Kong
- Worked in penetration test, code audit and threat analysis
- Interested in reverse engineering and malware analysis as well as programming ☺



Story begins ...>

At 2300

Hack the crimeware

Got a link

- http://pastie.org/pastes/888690 from www.malwaredomainlist.com

Its features

From the *pastie* link, it includes the following features:

- It is undetectable from anti-virus scanner
- Obfuscate the PDF payload randomly
- Checking whether the domain is on the blacklist
- Prevent Wepatweb, Jsunpack and other Javascript unpackers to decode the page.

- To guarantee high level of penetration and successful exploit, it could offer various exploits, which are shown below:
  - Adobe Acrobat Reader Exploits (including CVE-2010-0188)
  - JRE (GSB & SERIALIZE)
  - MDAC (IE)
  - MS09-032 (IE)
  - MS09-002 (IE)
  - CVE-2010-0806 (IE)

Aha … I love the evil feeling ☺

Mission 1: Try it out

- Understand and get to know how it works
- The only way is to grab a trial account

Social Engineering

- Add the contact in IM.
- Wait for reply

2 days later...

Replies and Conversation

- **6.1 Conversation with Crimepack "key person" via IM on 15 April 2010**
- 2:17:06 AM Buyer: Hi dude
- 2:17:10 AM Buyer: I come from Hong Kong
- 2:17:17 AM Buyer: I want to purchase the Crimepack.
- 2:17:26 AM Buyer: how can I try it out?
- 2:17:29 AM Buyer: what is the price/
- 2:17:39 AM Buyer: how to pay it?
- 2:17:44 AM Buyer: and any discount for me, dude?
- Changed status to Offline (2:18:53 AM)
- Changed status to Online (2:18:54 AM)
- 2:20:56 AM NEW VERSION 2.8.2 AVAILABLE NOW: what forum are u from?
- 2:21:06 AM Buyer: fourm?
- 2:21:09 AM Buyer: pastie.org
- 2:23:15 AM NEW VERSION 2.8.2 AVAILABLE NOW: and where did you find the pastie link?
- 2:23:40 AM Buyer: I have forgotten it for a while, dude, as I just search crimepack in Google.
- 2:24:09 AM Buyer: crimeware
- 2:26:07 AM NEW VERSION 2.8.2 AVAILABLE NOW: i see
- 2:26:29 AM NEW VERSION 2.8.2 AVAILABLE NOW: price is 400$, and you can pay with WebMoney (WMZ)
- 2:26:38 AM Buyer: 400 USD
- 2:26:41 AM Buyer: right?
- 2:26:43 AM NEW VERSION 2.8.2 AVAILABLE NOW: yes

- 2:26:54 AM Buyer: May I have to try it for at least a few days?
- 2:27:07 AM NEW VERSION 2.8.2 AVAILABLE NOW: yeah
- 2:27:55 AM Buyer: thanks,
- 2:28:09 AM Buyer: anything I need to obey or fulfill when I use the crimeware.
- 2:30:11 AM NEW VERSION 2.8.2 AVAILABLE NOW: what do you mean_
- 2:30:24 AM Buyer: i mean terms and conditions of using the crimeware.
- 2:31:31 AM NEW VERSION 2.8.2 AVAILABLE NOW: yeah terms of condition is don't share it, don't resell it and use it at your own risk
- 2:31:56 AM Buyer: with full access of installation, configuration documentation
- 2:32:17 AM Buyer: right?
- 2:32:25 AM Buyer: okay, thanks,
- 2:32:51 AM NEW VERSION 2.8.2 AVAILABLE NOW: you recieve the files, and a documentation how to install it yeah
- 2:32:56 AM Buyer: okay

- 2:33:07 AM Buyer: then may I be granted trial access right now?
- 2:33:28 AM Buyer: as I will travel to Japan soon, may I have the access for 5 days?
- 2:33:39 AM NEW VERSION 2.8.2 AVAILABLE NOW: yes
- 2:33:41 AM Buyer: I would like to try it out within coming 5-7 days?
- 2:33:51 AM Buyer: thanks, dude.
- 2:34:11 AM NEW VERSION 2.8.2 AVAILABLE NOW: i can setup a trial for you in 1 hour
- 2:34:22 AM Buyer: thank, mate
- 2:34:30 AM Buyer: it seems the featue is good
- 2:34:39 AM Buyer: may I enjoy any upgrade after purchase it?
- 2:35:14 AM NEW VERSION 2.8.2 AVAILABLE NOW: pack improvements are usually free
- 2:35:18 AM NEW VERSION 2.8.2 AVAILABLE NOW: first av cleaning is free
- 2:35:20 AM Buyer: good.
- 2:35:28 AM NEW VERSION 2.8.2 AVAILABLE NOW: 2 domain rebuilds are free
- 2:36:01 AM NEW VERSION 2.8.2 AVAILABLE NOW: what brought you interest in crimepack?
- 2:36:02 AM Buyer: may I set it up in my personal computer to try it out first before putting it to the domain?
- 2:36:17 AM Buyer: I would like to study how it works only
- 2:36:21 AM NEW VERSION 2.8.2 AVAILABLE NOW: the trial will be hosted on my server
- 2:37:09 AM Buyer: nice
- 2:37:11 AM NEW VERSION 2.8.2 AVAILABLE NOW: the pack will then be bound to a domain so if you redirect your domain to your personal computer then you can test it there
- 2:38:30 AM Buyer: thanks, mate.

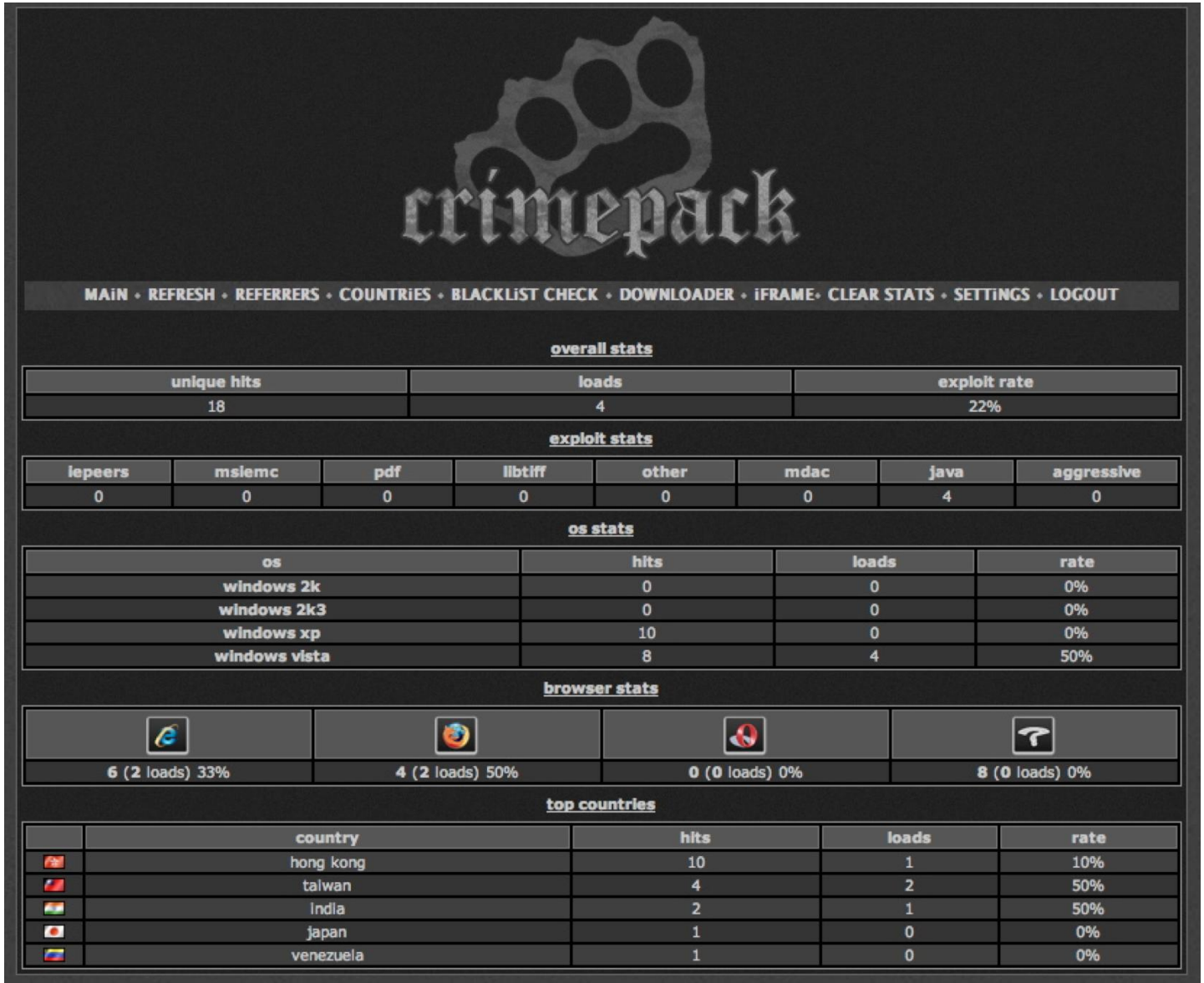
- 2:38:53 AM Buyer: then I would like to know how you have interest to make crimepack as well?
- 2:39:08 AM NEW VERSION 2.8.2 AVAILABLE NOW: what do you think?
- 2:39:12 AM Buyer: It is quite advanced indeed.
- 2:39:25 AM Buyer: to make $$$ to sponsor your research indeed.
- 2:40:02 AM NEW VERSION 2.8.2 AVAILABLE NOW: its all about making money
- 2:40:24 AM Buyer: I also want to be have such kungfu like you guys in the future.
- 2:42:26 AM NEW VERSION 2.8.2 AVAILABLE NOW: what kind of malware do you run?
- 2:42:46 AM Buyer: IE exploit
- 2:42:59 AM Buyer: or browser exploit.
- **2:43:41 AM NEW VERSION 2.8.2 AVAILABLE NOW: so your intensions of buying the exploit is not to spread your malware?**
- **2:44:27 AM Buyer: i am just studying over it**
- 2:46:24 AM Buyer: "use it at my own risk", right?
- 2:47:22 AM Buyer: Then I could try it out in an hour, couldn't I?
- 2:47:36 AM Buyer: For the web money account, do you have any more details for me?
- 2:51:44 AM NEW VERSION 2.8.2 AVAILABLE NOW: ?
- 2:51:58 AM Buyer: how can I transfer the money to you?
- 2:52:39 AM Buyer: i just used paypal in the past
- 3:03:33 AM Buyer: hi there?
- 3:04:04 AM Buyer: do you mind to drop me message once you have set the trial for me?
- 3:04:18 AM Buyer: this is my mail <MY EMAIL ADDRESS>

- 3:19:48 AM Buyer: Hello?
- **3:23:03 AM NEW VERSION 2.8.2 AVAILABLE NOW: i'm not interested to sell to security researchers**
- 3:24:16 AM Buyer: dude, i can't disclose too much to you right now becos it is proabably installed in China.
- 3:24:30 AM Buyer: our conversation is not encrypted
- 3:24:46 AM Buyer: there is no guarantee anyone sniffs our traffic.
- 3:25:32 AM Buyer: i could only disclose, i have been recruited to test on it before someone spread the malware.
- **3:27:13 AM Buyer: The boss behind does not want a single guy to undertake the whole/entire attack/malware spreading process, that's it**
- **3:27:32 AM Buyer: I don't know what he targets on neither.**
- **3:27:51 AM Buyer: i also just make money.**
- **3:28:56 AM Buyer: what do you think, dude?**
- **3:29:49 AM NEW VERSION 2.8.2 AVAILABLE NOW: http://87.98.218.204/cn/admin.php <removed admin account ID>/<removed passwd>**
- **3:29:51 AM NEW VERSION 2.8.2 AVAILABLE NOW: have fun**
- **3:29:52 AM NEW VERSION 2.8.2 AVAILABLE NOW: you got**
- **3:29:53 AM NEW VERSION 2.8.2 AVAILABLE NOW: 5 days**
- **3:29:58 AM Buyer: thanks, mate.**
- 3:30:08 AM Buyer: thanks for your understanding.
- **3:30:25 AM NEW VERSION 2.8.2 AVAILABLE NOW: if i see any attempts of sql injection i will remove it**
- **3:30:44 AM Buyer: sure, no problem, i just tried out the functions and feedback to the boss behind.**
- **3:30:57 AM Buyer: I will be the contact point to reach you to purchase.**
- 3:31:02 AM NEW VERSION 2.8.2 AVAILABLE NOW: ok
- 3:32:50 AM Buyer: I will have 1-2 mates from US to try out the function only.

- 3:49:50 AM NEW VERSION 2.8.2 AVAILABLE NOW: you tested with firefox?
- 3:50:12 AM Buyer: yeah
- 3:50:19 AM Buyer: and Chorme
- 3:50:43 AM NEW VERSION 2.8.2 AVAILABLE NOW: try now
- 3:51:02 AM NEW VERSION 2.8.2 AVAILABLE NOW: if 'enable bad traffic' is not checked it will not allow Chrome and other browsers visit the page
- 3:51:05 AM NEW VERSION 2.8.2 AVAILABLE NOW: only IE, FF, OP
- 3:51:38 AM NEW VERSION 2.8.2 AVAILABLE NOW: also its because you are visiting with a Mac, it is for Windows Only
- 3:52:19 AM Buyer: okay
- 4:50:01 AM Buyer: hi dude
- 4:50:13 AM Buyer: I have tried http://87.98.218.204/cn/index.php again in IE
- 4:50:16 AM Buyer: but it faile.
- 4:50:19 AM Buyer: failed
- 4:50:27 AM Buyer: Not Found message is shown.
- 4:54:18 AM NEW VERSION 2.8.2 AVAILABLE NOW: because you already visited it
- 4:54:30 AM NEW VERSION 2.8.2 AVAILABLE NOW: if your ip is already in the database it will show a 404 next time you visit
- 4:54:35 AM NEW VERSION 2.8.2 AVAILABLE NOW: clear the stats and you can visit again
- 4:54:52 AM NEW VERSION 2.8.2 AVAILABLE NOW: unnessicery to have duped victims

- 3:33:14 AM Buyer: do you have any readme/docs for me?
- 3:39:18 AM NEW VERSION 2.8.2 AVAILABLE NOW: go to 'settings' and upload exe
- 3:39:21 AM NEW VERSION 2.8.2 AVAILABLE NOW: send traffic to http://87.98.218.204/cn/index.php
- 3:47:52 AM Buyer: dude
- 3:47:59 AM Buyer: it is not found;
- 3:48:00 AM Buyer: http://87.98.218.204/cn/index.php
- 3:48:21 AM Buyer: do you have a handle for me call you?
- 3:48:21 AM NEW VERSION 2.8.2 AVAILABLE NOW: what browser you visit with?
- 3:48:25 AM Buyer: Firefox
- 3:48:51 AM NEW VERSION 2.8.2 AVAILABLE NOW: working for me
- 3:49:06 AM Buyer: Not Found
- The requested URL / was not found on this server.
-

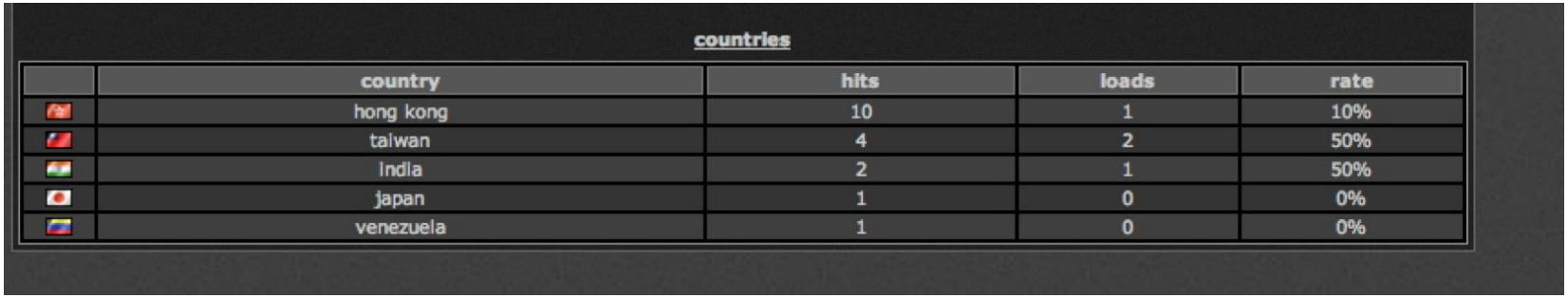
Main Menu


crimepack
MAiN • REFRESH • REFERRERS • COUNTRiES • BLACKLiST CHECK • DOWNLOADER • iFRAME• CLEAR STATS • SETTiNGS • LOGOUT
overall stats
unique hits
loads
exploit rate
18
4
22%
exploit stats
lepeers
mslemc
pdf
libtiff
other
mdac
java
aggressive
0
0
0
0
0
0
4
0
os stats
os
hits
loads
rate
windows 2k
0
0
0%
windows 2k3
0
0
0%
windows xp
10
0
0%
windows vista
8
4
50%
browser stats
6 (2 loads) 33%
4 (2 loads) 50%
0 (0 loads) 0%
8 (0 loads) 0%
top countries
country
hits
loads
rate
hong kong
10
1
10%
taiwan
4
2
50%
india
2
1
50%
japan
1
0
0%
venezuela
1
0
0%

Referrer


MAiN • REFRESH • REFERRERS • COUNTRiES • BLACKLiST CHECK • DOWNLOADER • iFRAME• CLEAR STATS • SETTiNGS • LOGOUT
referrer
referrer
hits
loads
rate
www.facebook.com
4
0
0%

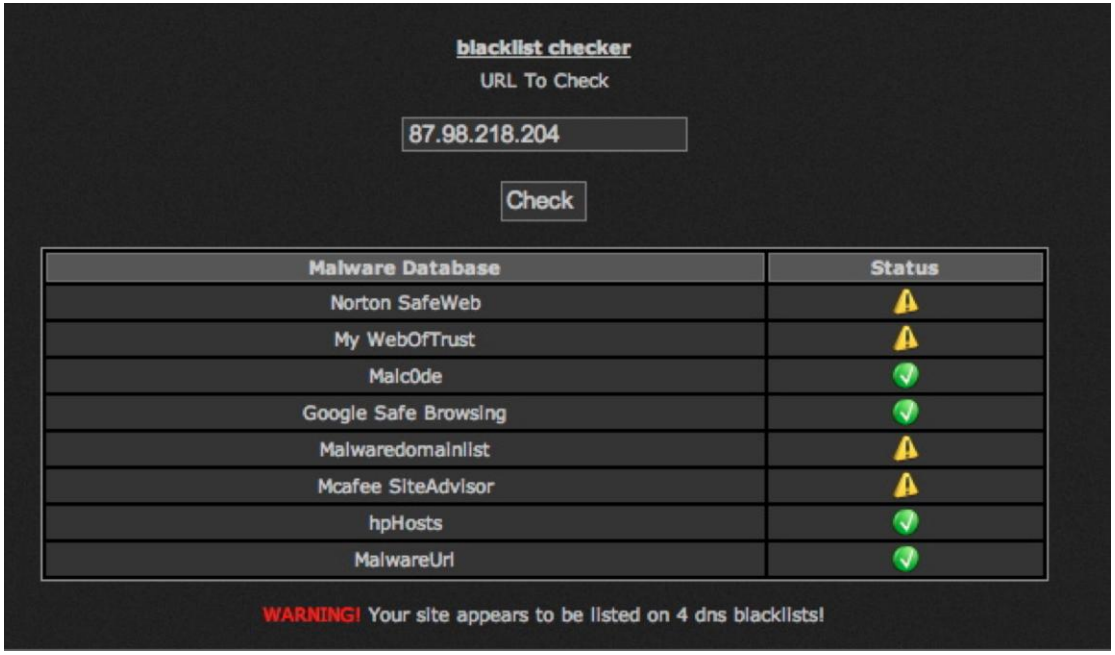
Origin of countries



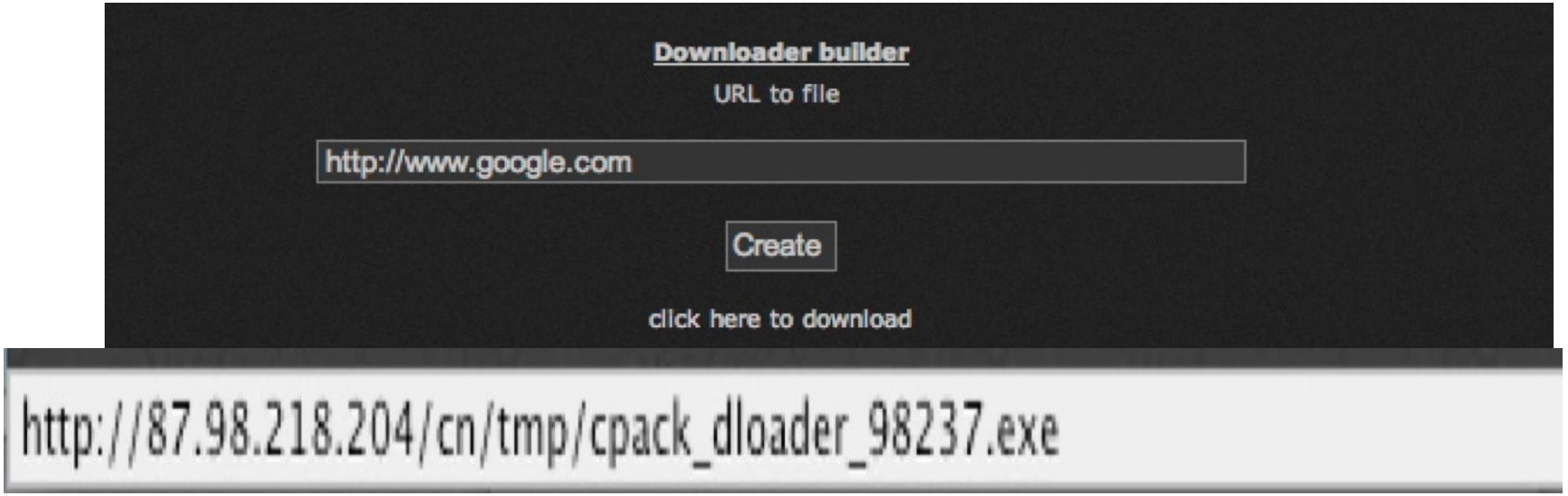
countries

	country	hits	loads	rate
	hong kong	10	1	10%
	taiwan	4	2	50%
	India	2	1	50%
	japan	1	0	0%
	venezuela	1	0	0%

Blacklist Check



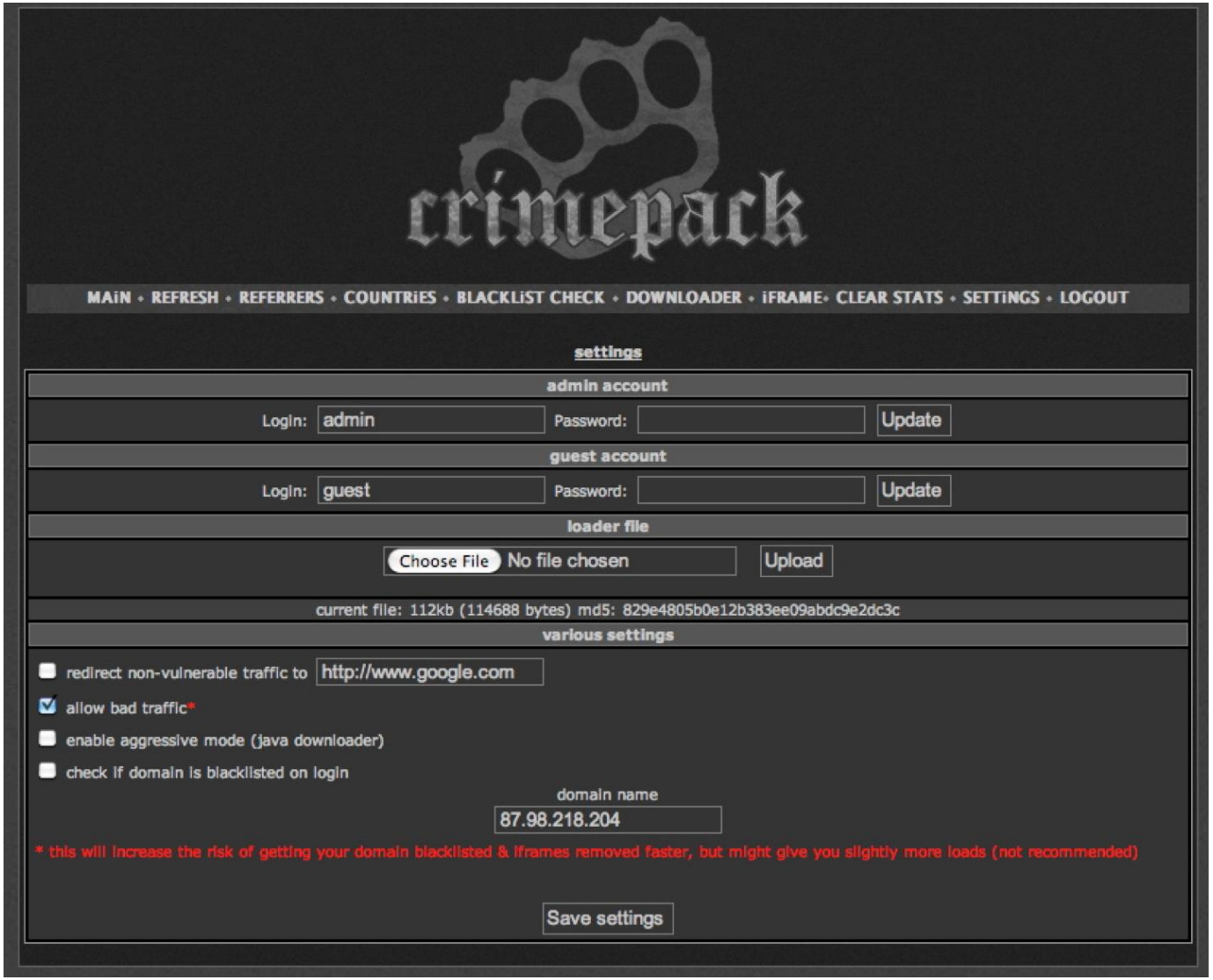
Build a Downloader



Clear Statistics

- **Clear Stats**
- It allows the administrator to clear up all statistics of latest malware deployment.

Setting?

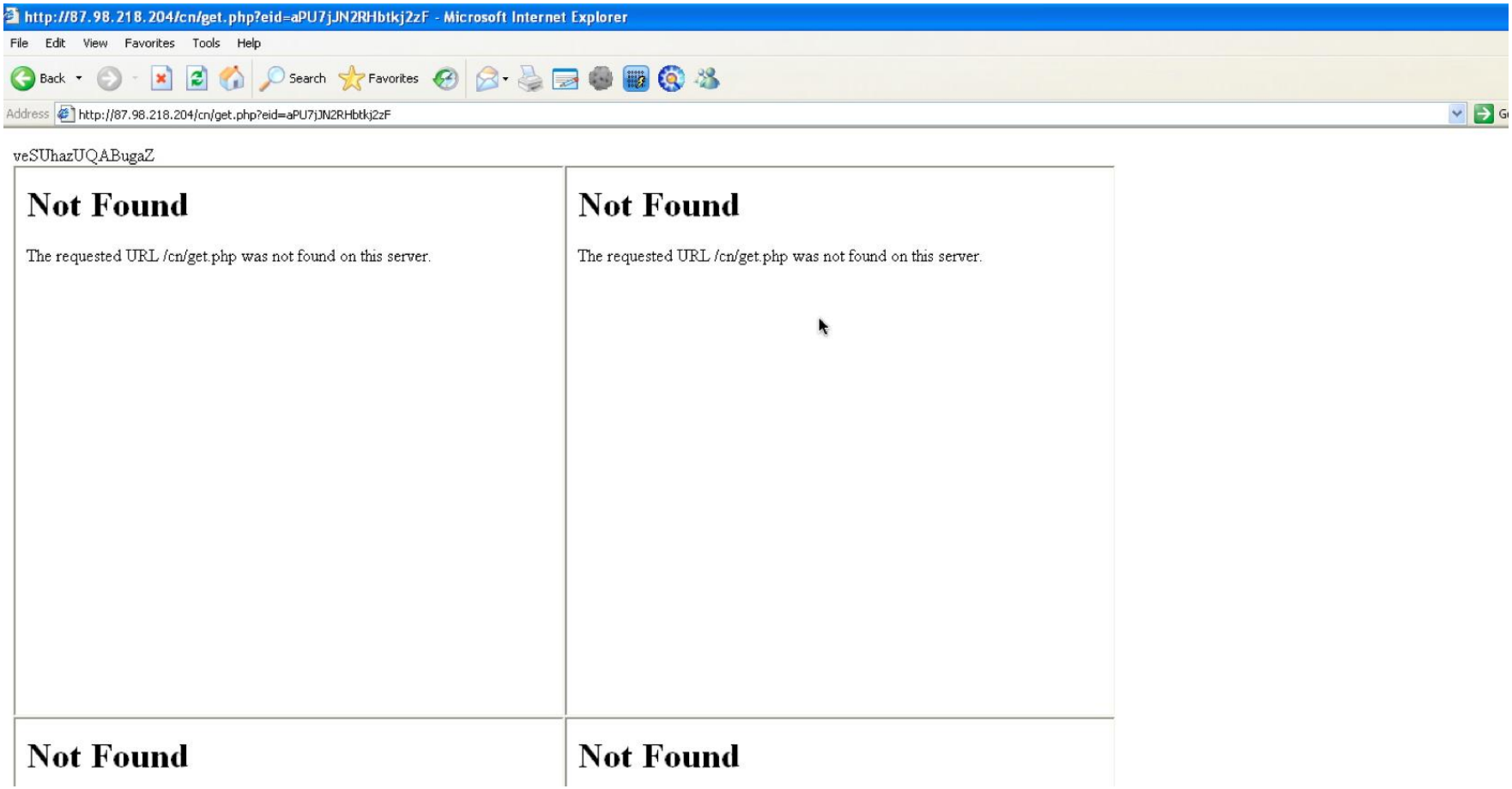

crimepack
MAIN • REFRESH • REFERRERS • COUNTRIES • BLACKLIST CHECK • DOWNLOADER • iFRAME• CLEAR STATS • SETTINGS • LOGOUT
settings
admin account
Login: admin
Password:
Update
guest account
Login: guest
Password:
Update
loader file
Choose File
No file chosen
Upload
current file: 112kb (114688 bytes) md5: 829e4805b0e12b383ee09abdc9e2dc3c
various settings
redirect non-vulnerable traffic to
http://www.google.com
allow bad traffic*
enable aggressive mode (java downloader)
check if domain is blacklisted on login
domain name
87.98.218.204
* this will increase the risk of getting your domain blacklisted & iframes removed faster, but might give you slightly more loads (not recommended)
Save settings

Mission 2: Analysis and Deobfuscation

The site is ready

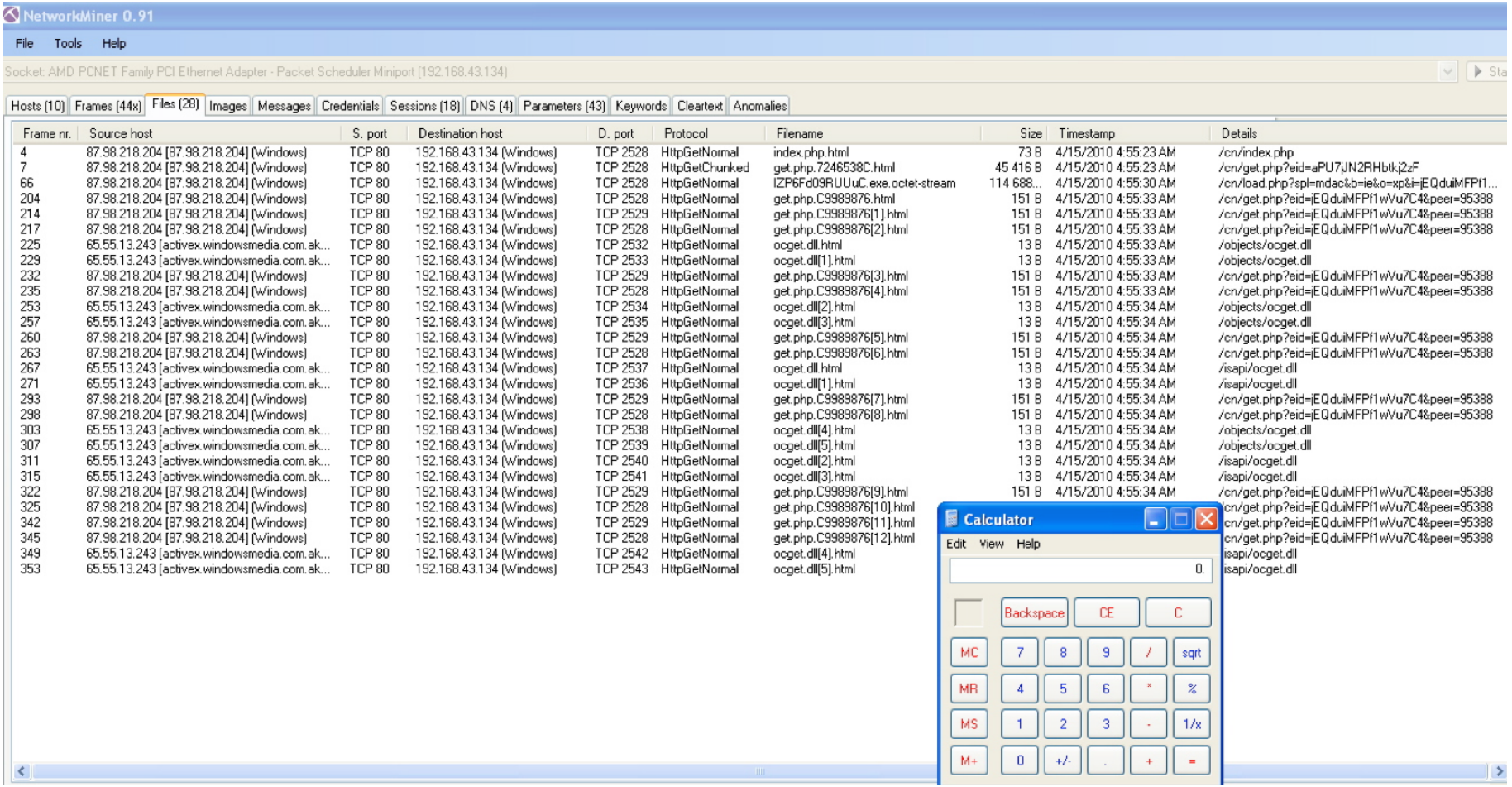
- **http://87.98.218.204/cn/index.php,**
- **Aha, it is the seller's server ☺**
- **I have uploaded a payload, simply calc.ex**
  - **Payload characteristic**
  - **Size:** 112kb (114688 bytes)
  - **md5:** 829e4805b0e12b383ee09abdc9e2dc3c

Visit the site in VM



Pwned

- 114KB executable has been downloaded



How about automated scan?

- Wepaweb: **FAILED**

How about automated scan?

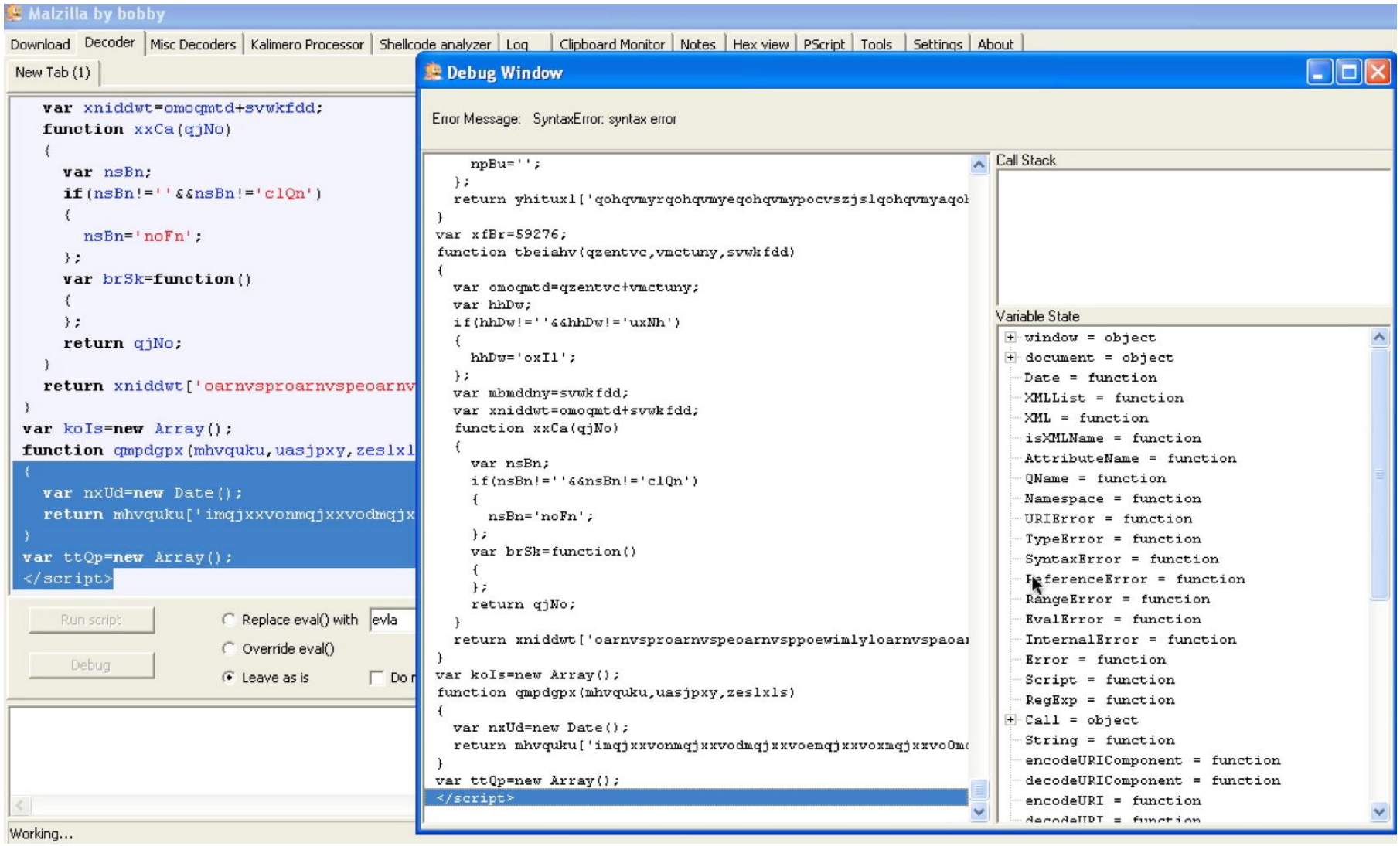
- **Jsunpack: Yeah!**
- For more details and payload download, it could be found from the following URL: http://jsunpack.jeek.org/dec/go?report=f5b4710bb96e4b9d4ea440164c2d70120299c3a3
- The password is “infected”.

More conversation

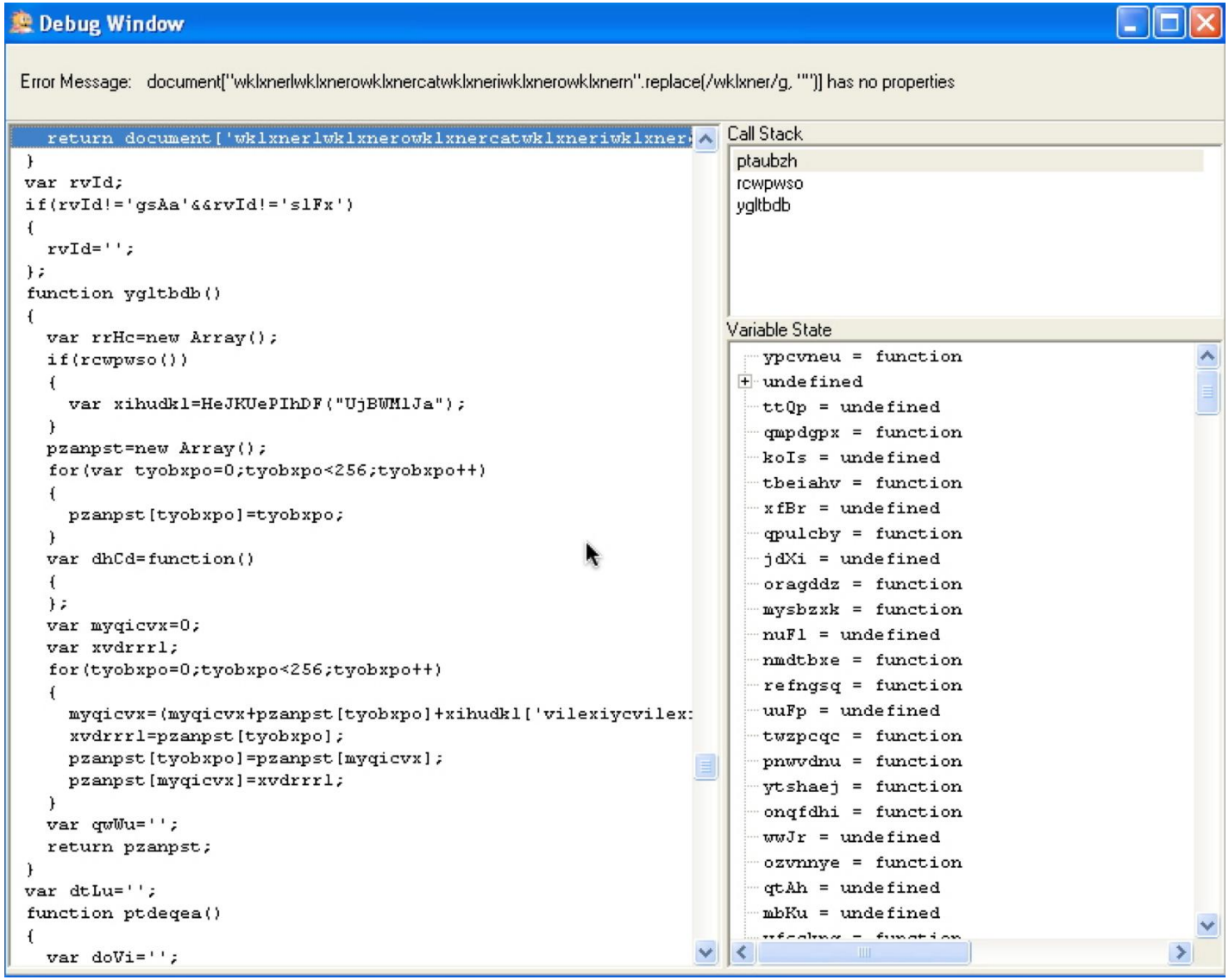
- 1:01:38 AM Buyer: does it support more obfuscation.
- 1:01:54 AM Buyer: Wepaweb cannot analyze it.
- 1:02:04 AM Buyer: however, Jsunpack could do it.
- 1:02:37 AM Crimepack 3.0-Delta available: crimepack itself does not make any other obfuscation due to Kaspersky detecting most of them so i figured out a way how to not get it detected and thats how its implemented
- 1:02:53 AM Crimepack 3.0-Delta available: i can take a look at jsunpack later, i've bypassed it quite a few times already
- 1:04:36 AM Crimepack 3.0-Delta available: anyways im working on some improvements on the pack, ina few days i can give you another evaluation panel so you can try out the new version
- 1:04:52 AM Buyer: that's nice
- 1:05:38 AM Buyer: may be, you could allow us to import some exploits
- 1:08:57 AM Crimepack 3.0-Delta available: yes i'm planning to add a few exploits for AIM (not the newest though) that hopefully will have some effect on US traffic, along with the Firefox 3.5 exploit, and a few activex control exploits
- 1:09:34 AM Crimepack 3.0-Delta available: and i'm also thinking about creating kind of a development framework so you can include your own exploits on the fly and enable/disable them

Manual” Kungfu

Syntax Error?



Ops, Document has no properties



Declare a variable type for *zelslxls* instead of id name in

- // Original:

```
<div id="zeslxls”
style="display:none;">eS8kz…</d
iv>
```

- `var zelslxls = “……”;`

After executing the replace function, it is *document.getElementById("zeslxls").innerHTML*, we simply put it as "*zelslxls*" as it is no longer an id of tag.

- //Original:

```
var
mzmiycr=HeJKUePIhDF(document['pndqsqp
gpndqsqpepndqsqptpndqsqpEpndqsqplpndq
sqpepndqsqpmpndqsqpepndqsqpnpndqsqptp
ndqsqpBpndqsqpypndqsqpIpndqsqpdpndqsq
p'.replace(/pndqsqp/g,'')]("zeslxls")
.innerHTML);
```

- // Deobfuscated and zeslxls is not an ID of but it is defined as a variable.

```
var mzmiycr=HeJKUePIhDF(zeslxls);
```

Replace the executed result “search” with [...]

- //Original:

```
znknvsh['wklxnerswklxnerewklxnerarwklxnerch'.replace(/wklxner/g,'')](zdiubxv);
```

- ```
var mcstfpj=znknvsh.search(zdiubxv);
```
```

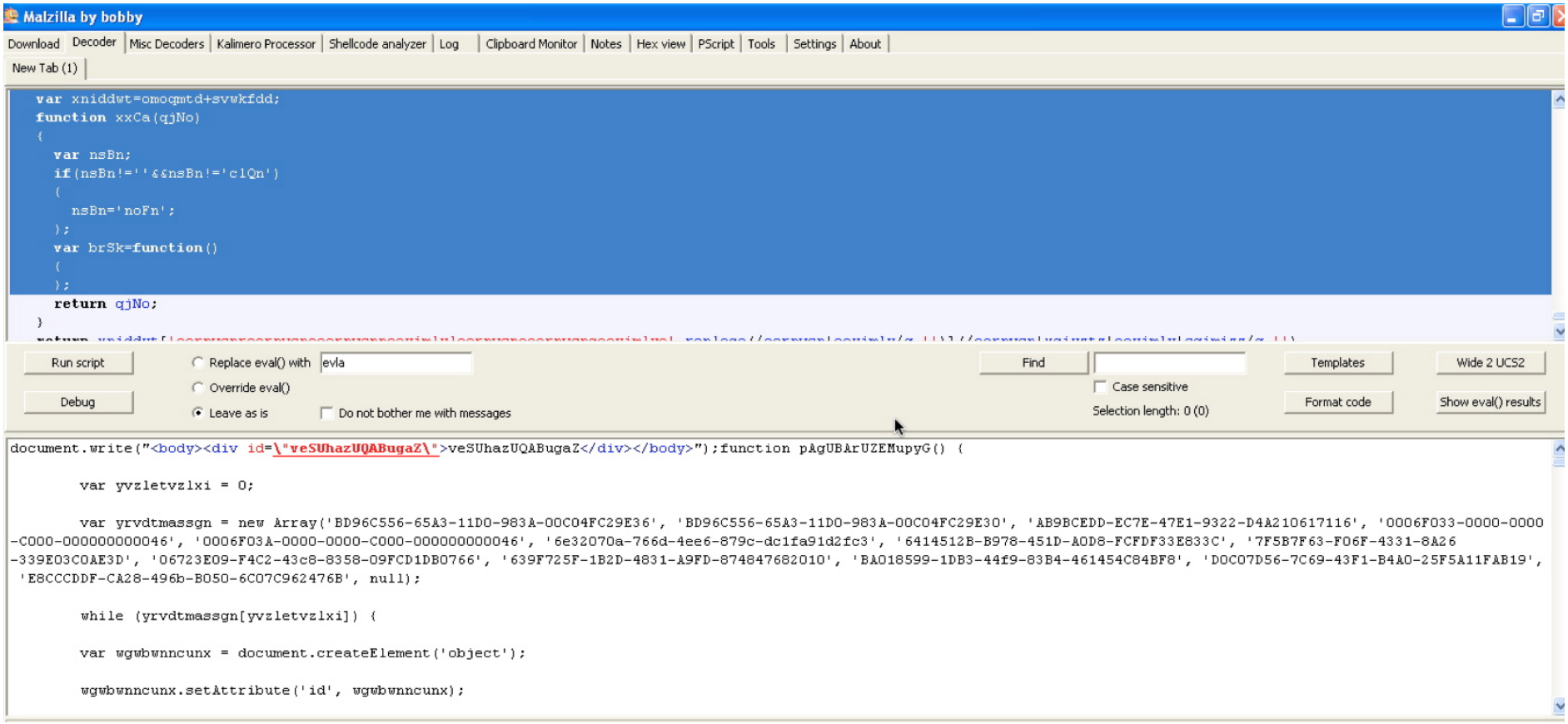
Replace the executed result *document.location.herf* with any URL.

- //Original:

```
return
document['wklxnerlwklxnerowklxnerc
atwklxneriwklxnerowklxnern'.replac
e(/wklxner/g,'')].href;
```

- `return "http://www.google.com";`

Yeah!


Malzilla by bobby
Download
Decoder
Misc Decoders
Kalimero Processor
Shellcode analyzer
Log
Clipboard Monitor
Notes
Hex view
PScript
Tools
Settings
About
New Tab (1)
var xniddwt=omocqmtd+svwkfdd;
function xxCa(qjNo)
{
var nsBn;
if(nsBn!=''&&nsBn!='clQn')
{
nsBn='noFn';
};
var brSk=function()
{
};
return qjNo;
}
Run script
Debug
Replace eval() with
evla
Override eval()
Leave as is
Do not bother me with messages
Find
Case sensitive
Selection length: 0 (0)
Templates
Format code
Wide 2 UCS2
Show eval() results
document.write("<body><div id=\"veSUhazUQABugaZ\">veSUhazUQABugaZ </body>");function pAgUBArUZEMupyG() {
var yvzletvzlxi = 0;
var yrvdtmassgn = new Array('BD96C556-65A3-11D0-983A-00C04FC29E36', 'BD96C556-65A3-11D0-983A-00C04FC29E30', 'AB9BCEDD-EC7E-47E1-9322-D4A210617116', '0006F033-0000-0000-C000-000000000046', '0006F03A-0000-0000-C000-000000000046', '6e32070a-766d-4ee6-879c-dc1fa91d2fc3', '6414512B-B978-451D-A0D8-FCFDF33E833C', '7F5B7F63-F06F-4331-8A26-339E03C0AE3D', '06723E09-F4C2-43c8-8358-09FCD1DB0766', '639F725F-1B2D-4831-A9FD-874847682010', 'BA018599-1DB3-44f9-83B4-461454C84BF8', 'D0C07D56-7C69-43F1-B4A0-25F5A11FAB19', 'E8CCCDDF-CA28-496b-B050-6C07C962476B', null);
while (yrvdtmassgn[yvzletvzlxi]) {
var wgwbwnncunx = document.createElement('object');
wgwbwnncunx.setAttribute('id', wgwbwnncunx);

Put it more simple

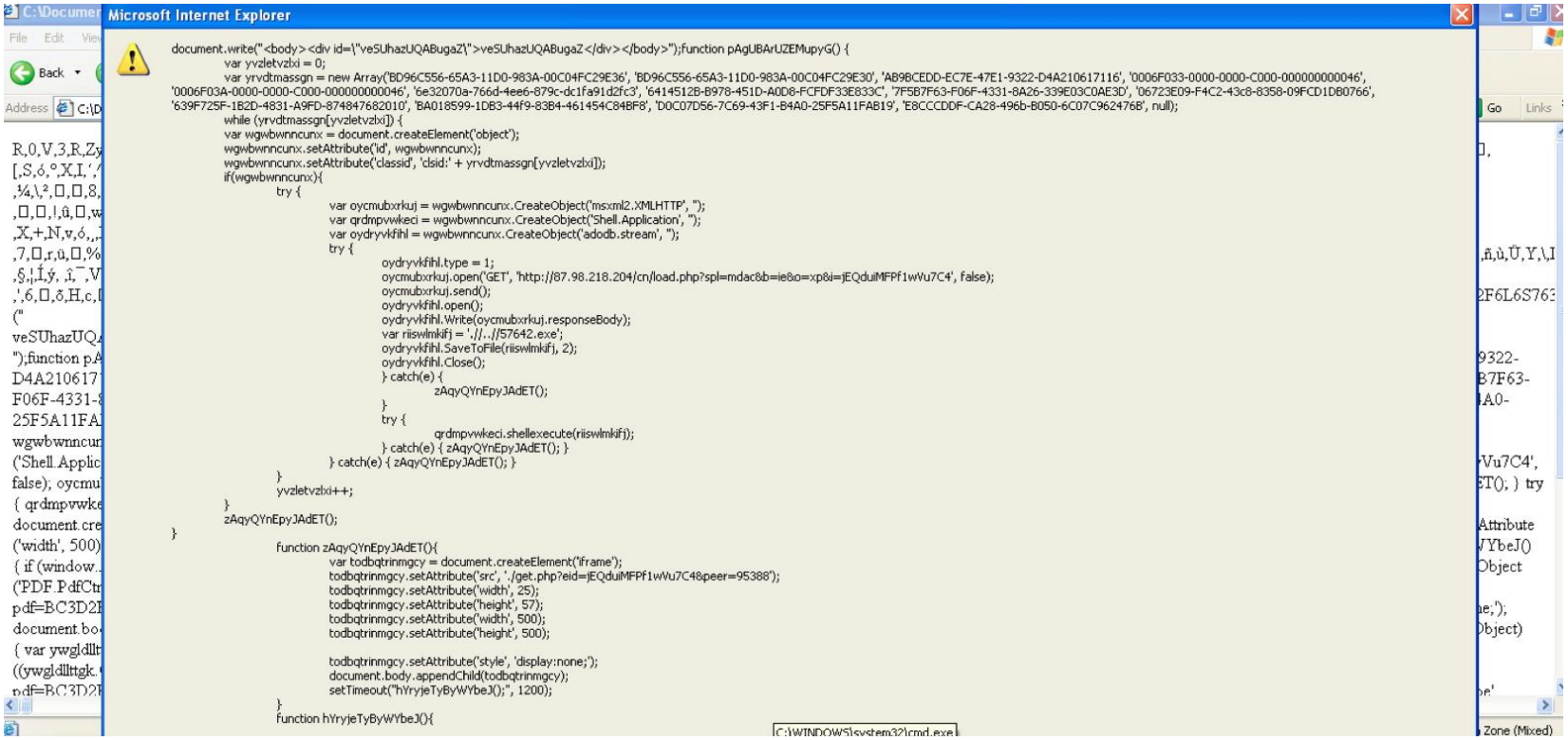
- We have put a document.write and alert on the variable in the following code section with for-loop:

```
for (i=0;i<qfnynws.length;i+=2) {

  mbtnpoq+=oragddz(ptdbrww(qfnynws[yaunsut[vfsc
  kpg('vvbciksrtwlculxe','vvbcikspqioqrfjltwlcu
  lxa','twlculxcvvbcikse')](/AJ/g,'')](i,zexegx
  w),ptdeqea()));
}

document.write(mbtnpoq);
alert(mbtnpoq);
```

We could still get the result



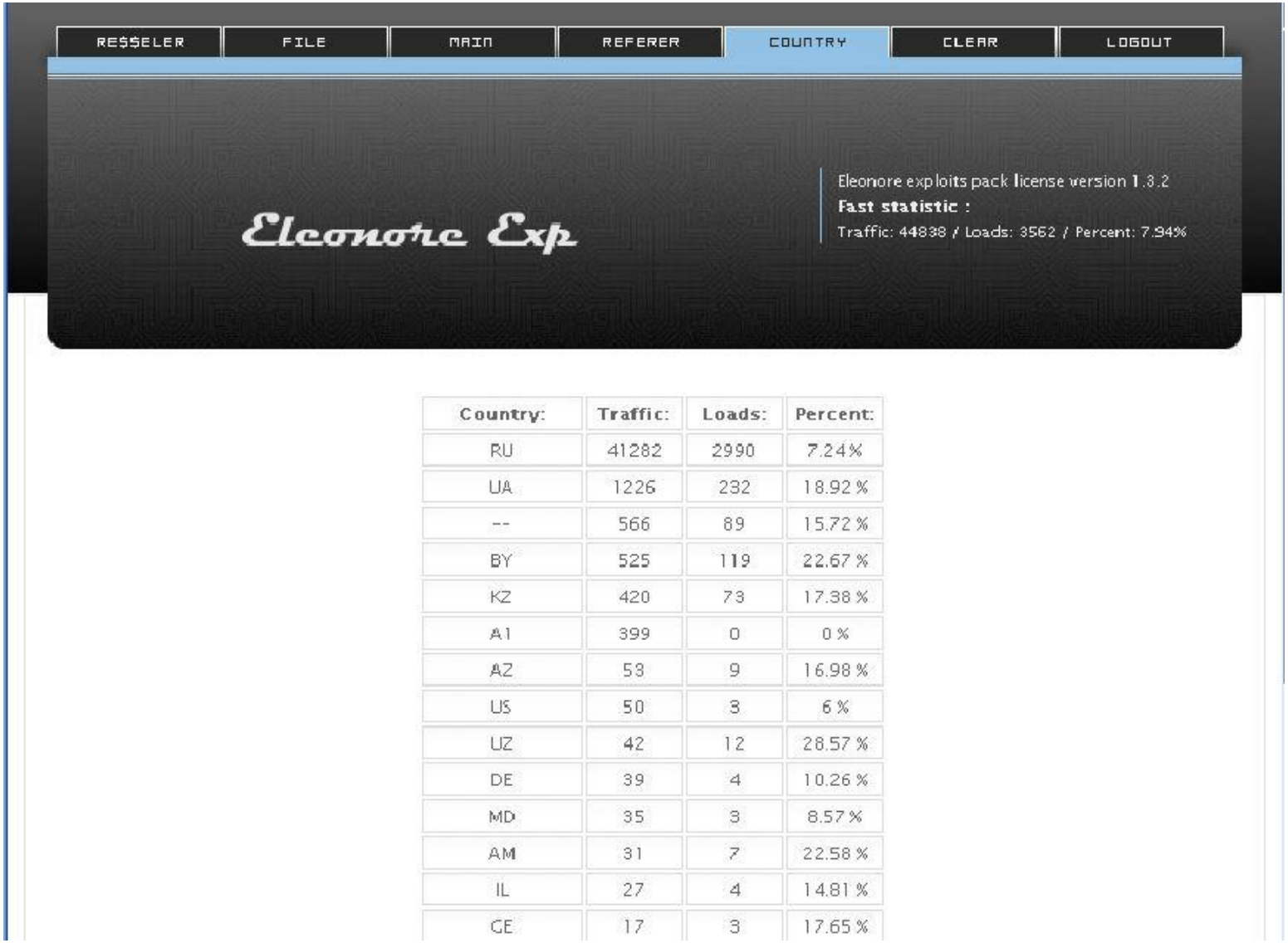
Mission 3: Let’s sum up

Exploit-based Crimeware

- Existing exploits
- Bundled attack
- Bypassing deobfuscation
- Bypassing AV
- Checking whether it is blacklisted.

….

Eleonore Browser Exploit Kit



Country:	Traffic:	Loads:	Percent:
RU	41282	2990	7.24%
UA	1226	232	18.92 %
--	566	89	15.72 %
BY	525	119	22.67 %
KZ	420	73	17.38 %
A1	399	0	0 %
AZ	53	9	16.98 %
US	50	3	6 %
UZ	42	12	28.57 %
DE	39	4	10.26 %
MD	35	3	8.57 %
AM	31	7	22.58 %
IL	27	4	14.81 %
GE	17	3	17.65 %

Browsers:	Traffic:	Loads:	Percent:
Bots	18	0	0
Chrome 0.3	2	0	0
Chrome 1.0	6	1	16.67
Chrome 2.0	7	3	42.86
Chrome 3.0	211	27	12.8
Chrome 4.0	20	1	5
FireFox 0.10	1	0	0
FireFox 0.8	1	0	0
FireFox 1.0	6	0	0
FireFox 1.0.1	1	1	100
FireFox 1.0.2	1	0	0
FireFox 1.0.3	1	0	0
FireFox 1.0.4	3	2	66.67
FireFox 1.0.6	3	0	0
FireFox 1.0.7	17	0	0
FireFox 1.5	4	1	25
FireFox 1.5.0	64	0	0
FireFox 1.6a1	1	0	0
FireFox 2.0	18	0	0
FireFox 2.0.0	507	0	0
FireFox 3.0	163	0	0
FireFox 3.0.1	283	1	0.35

http://krebsonsecurity.com/2010/01/a-peek-inside-the-eleonore-browser-exploit-kit/

GOLOD

http://malwareint.blogspot.com/2010/03/ipack-y-golod-new-on-scene-crimeware.html

iPack

Main | Referef | Country | Clear | Logout

Main Statistic

Operations System	Traffics / Loads / Percent
Windows XP	590 / 60 / 10.17 %
Windows Vista	41 / 4 / 9.76 %
Other	32 / 0 / 0 %
Windows 7	31 / 1 / 3.23 %
Windows 2000	13 / 0 / 0 %
Windows 95	11 / 0 / 0 %
Windows 98	9 / 0 / 0 %
Windows 2003	3 / 0 / 0 %
Windows ME	1 / 0 / 0 %
Browsers	**Traffics / Loads / Percent**
+ Firefox	**151 / 0 / 0 %**
Firefox	151 / 0 / 0 %
+ MSIE	**364 / 45 / 12.36 %**
MSIE 4	3 / 0 / 0 %
MSIE 5	27 / 0 / 0 %
MSIE 6	173 / 32 / 18.5 %
MSIE 7	97 / 9 / 9.28 %
MSIE 8	64 / 4 / 6.25 %
+ Opera	**177 / 19 / 10.73 %**
Opera	177 / 19 / 10.73 %
+ Other	**36 / 1 / 2.78 %**
Other	36 / 1 / 2.78 %
+ WebTV	**3 / 0 / 0 %**
WebTV	3 / 0 / 0 %
>>> TOTAL <<<	**> 731 / 65 / 8.89 % <**

Botnet-based Exploit Kit

- Spyeye
  - Made in Russia
  - **Formgrabbing** (an advanced keylogging method of capturing web form data) supporting Firefox, IE, Maxthon and Netscape.
  - **CC Autofill** (A module that, basically, automates the process of credit card frauds, and gives money to the owner)
  - **PHP-MYSQL Administration Panel**
  - Daily **backup of the database** via e-mail
  - **Exe String-Sources encryption**
  - **FTP Grabbing** (Total Commander, Notepad++, FileZilla, and others)
  - **POP3 Grabbing**
  - **Invisible in processes list, hidden file, invisible in autorun** (registry)

From:http://malwareint.blogspot.com/2010/01/spyeye-new-bot-on-market.html

Spy Eye v1.0

2009
12/28
22:35:20

Find !NFO | Statistic | Settings

3646 k
+54882

Get $tati$tic

Get hosts

Day for statistic :	28/12/2009
Limit :	100

submit

host	count	[controls]
www.google.com	1021	
www.delmarlearning.com	431	

Страница на http://www.microsoft-windows-security.com co...

Do you really want to ban this host (www.google.com) ?

OK | Отмена

			Count		info]	
00	2009-10-19 14:13:42	2009-11-10 00:13:42	25			
01	2009-10-27 14:23:17	2009-11-10 00:23:17	14			

Bots with cards for Global task # 301

Restart]	[New time]	ID Task	Planned Time	Begin Time	End Time	E-Mail	Message Log	Client's info	Id Bot
don't		4102	2009-10-27 17:08:53	2009-10-27 17:09:10	2009-10-27 17:15:52	trucnguyen82 @newhampshire.usa.com		6.0.6000 8.0.6001.18865 User	
don't		4104	2009-10-28 09:14:53	2009-10-28 09:15:22	2009-10-28 09:16:35	markusp28 @tvstar.com			
don't		4106	2009-10-29 19:03:29	2009-10-29 19:03:43	2009-10-29 19:05:43	valllerip34 @delhimail.com			
don't		4108	2009-10-30 05:52:05	2009-10-30 05:53:25	2009-10-30 05:54:52	paddybaby0242 @sister.com		5.1.2600 8.0.6001.18702 Admin	
don't	2009-10-10 20:23:53	4113	2009-10-31 10:37:05	2009-10-31 13:06:51	2009-10-31 13:08:17	jcropp18 @hour.com		5.1.2600 6.0.2800.1106 Admin	
don't		4116	2009-11-01 15:22:05	2009-11-01 15:27:35	2009-11-01 15:29:01	modaparkavenue76 @myself.com			
don't		4117	2009-11-02 04:28:41	2009-11-02 04:33:09		velicajames29 @kittymail.com	ERROR		
		4120	2009-11-03 10:50:17	2009-11-03 13:53:35		gregorysmith2 @atheist.com	ERROR	5.1.2600 7.0.5730.11 Admin	
don't		4122	2009-11-04 07:46:05	2009-11-04 14:00:16	2009-11-04 14:01:53	hendessi142 @seductive.com		5.1.2600 7.0.5730.13 Admin	
	2009-12-21 08:50:41	4133	2009-11-04 23:52:05	2009-12-22 07:14:57		tcdalessandro95 @alaska.usa.com			

Final Weapon: 0-Day Browser Exploit Kit

- Impassion Framework
  - I try to get an trial account but failed.
  - Provide 0-day exploits in IE and PDF monthly update.
  - They claim they have the largest market share!
  - 1400 EUROS/month!
  - Features: http://malwareview.com/index.php?topic=712.0
  - Watch the video from here:
    - http://www.youtube.com/watch?v=F4J3SeFkzXg

We offer a new Browser Exploitation Kit (bep) -> Impassioned Framework !!

CLICK HERE TO WATCH THE VIDEO

BROWSERS / OS AFFECTED:

- Chrome
- Firefox
- Msie 6
- Msie 7
- Msie 8
- Opera
- Safari

- Windows x

- Unix and OS X NON AFFECTED.

EXPLOITS INCLUDED:

We currently made tests using only the best exploits currently available, however any exploit may seen in other pack can be added into the system and will be functional.

- MS09_002
- MS09_043
- MS Dshow
- iepeers.dll
- Firefox escape
- Firefox CompareTo
- Java Calendar
- Adobe Reader Lib
- Adobe Reader newPlayer
- Adobe Flash 9
- Adobe Flash 10

We will use regular founds to buy exploits in 0day condition, and research them as well.

Hmmm...

- Exploit kit could automate the threat propagation
- You simply pay it and use it, it is user friendly.
- Easy to keep track of the infection
- Allow deploy your own exploit
- Law and rule has never made it clear whether crimeware is illegal or not.

Bonus stage ☺

Mission 4: Exploit the crimeware

Google hacking or Search Malware List

- http://www.malwaredomainlist.com/mdl.php?search=pack&colsearch=All&quantity=50
- http://www.malwaredomainlist.com/mdl.php?search=kit&colsearch=All&quantity=50

Scan over them!

- NMAP
- Free web tools
- SQL injection
- Directory traversal

Hack them?!

- Hack them down…(hahaha, own them for justice?! Dude, unless your police force allows you to do it)

“All that is necessary for the triumph of evil is that good men do nothing.”
- Edmund Burkle

Thank you for listening

- You could reach me for the slide and a short paper about it at darkfloyd@vxrl.org