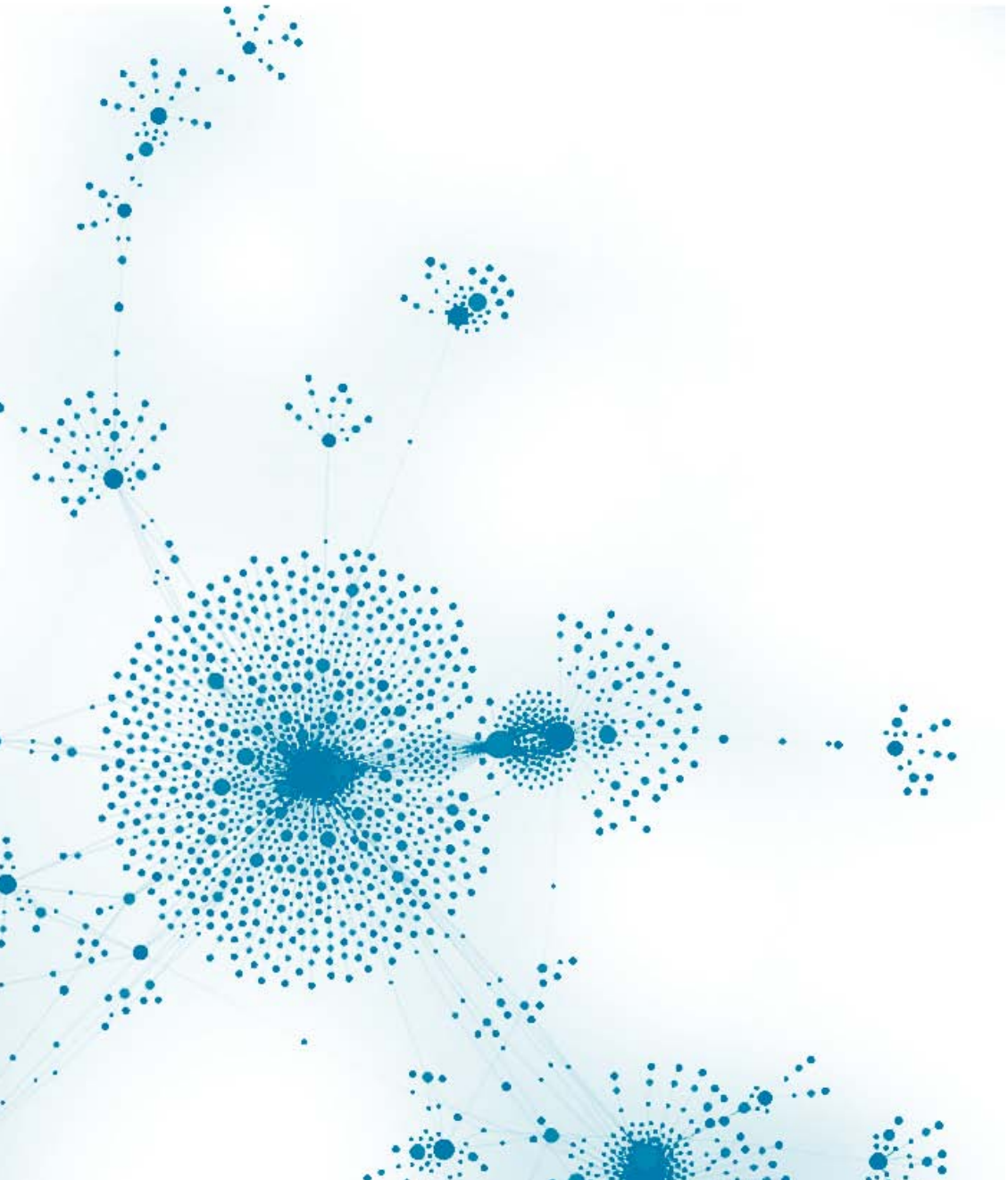
The many faces of Gh0st Rat

Plotting the connections between malware attacks

Snorre Fagerland, Principal Security Researcher
Norman ASA



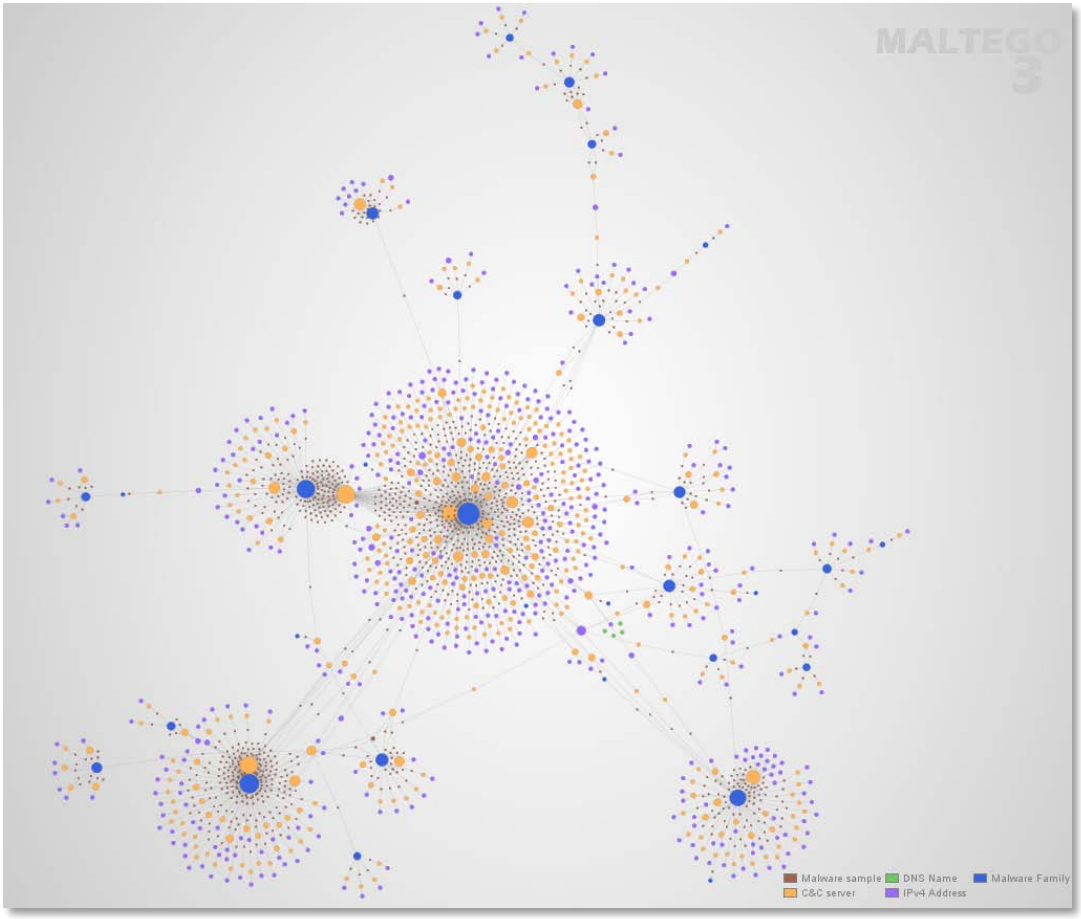
Content

Introduction

Gh0st Rat is a well-known Chinese remote access trojan which was originally made by C.Rufus Security Team several years ago. Just as with other well-featured "off-the-shelf" trojans like Poison Ivy, Hupigon and DarkComet it has been used by all sorts of people – from the script kiddie next door to resourceful targeted attack actors (1)

Cybercriminals use off-the-shelf malware not only because it's easy and cheap. They also use it because it's hard to track. Anybody could use this malware, so the criminal could be anybody. *However*, this changes somewhat when they start modifying the code. The malware now becomes somewhat attributable and can be connected to known cases and criminal groups. This document is the result of examining selected common traits between some 1200+ Gh0st Rat program files (samples) with the help of Maltego, a tool to visualize data connections. The samples were processed by us in a timeframe of approximately six months, from August 2011 to February 2012.

In this study we attempt to map out what logical connections do exist between different Gh0st botnet campaigns. This is important because it gives an indication of the scale of operation and sometimes what the aims of the campaigns are, and this can be valuable for risk analysis. Additional data produced by the study may be used for risk mitigation.



The variants

The Gh0st Rat source code (version 3.6) is freely available on the Internet, something that has made it quite popular and sparked a multitude of modifications. The resulting trojan can be hard to recognize as Gh0stRat, as attackers ditch various parts of the code that they don't need and add other functionality. In addition, the trojan is packaged in different ways – standalone, glued together with other files, included in self extracting archives. It is frequently obfuscated and compressed.

As a result of all this, antivirus naming is variable, to put it mildly. Most antivirus detections today are automatically generated, resulting in names thought out by machines. Quick, but containing information only machines find interesting.

The most stable indicator of being faced with a Gh0stRat is its network communication. It is well documented and quite distinctive, as it always begins with a "magic word" which in its default configuration is "Gh0st" – thus Gh0st Rat. Below is a typical packet (content data blurred)

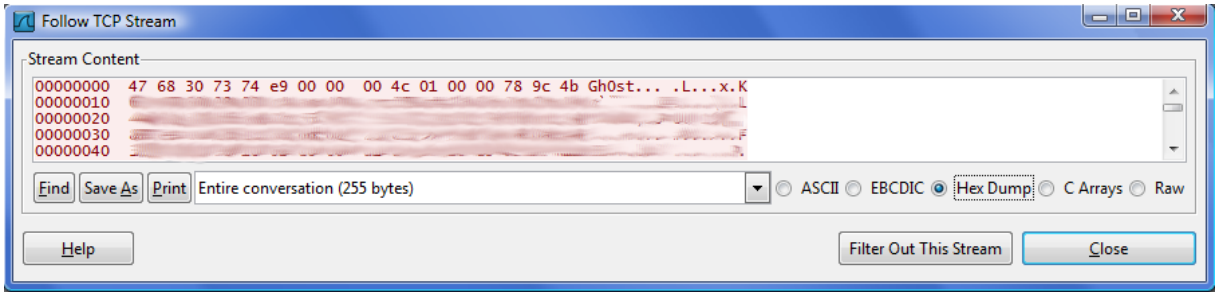


Fig 1 The fields are magic identifier ('Gh0st'), size of packet, size of uncompressed packet, and lz-compressed data containing information about the compromised computer.

This magic tag is very easy to spot in network traffic, so the bad guys have come up with a countermeasure. They use *other* magics. I searched our in-house Malware Analyzer G2 (MAG2) pcaps for network traffic that matched the Gh0st packet format, and this showed about 50 different magics from the last few months. There are many more in existence – some are shown in Table 2, but as we had no traffic data on these, they were not investigated.

```
7hero, Adobe, B1X6Z, BEiLa, BeiJi, ByShe, FKJP3, FLYNN, FWAPR, FWKJG,
GWRAT, Gh0st, GOLDt, HEART, HTTPS, HXWAN, Heart, IM007, ITore, KOBBX,
KrisR, LUCKK, LURK0, LYRAT, Level, Lover, Lyyyy, MYFYB, MoZhe, MyRat,
OXXMM, PCRat, QWPOT, Spidern, Tyjhu, URATU, W0LFKO, Wangz, Winds, World,
X6RAT, XDAPR, Xjjhj, ag0ft, attac, cb1st, https, whmhl, xhjyk
```

Table 1. Gh0st magic tags used in this paper

```
00000, ABCDE, apach, Assas, Blues, chevr, CHINA, cyl22, DrAgOn EXXMM,
Eyes1, Gi0st, GM110, Hello, httpx, kaGni, light, LkxCq, lvxYT, Naver,
NIGHT, NoNul, Origi, QQ_124971919, Snown, SocKt, Super, Sw@rd, v2010,
VGTLS, wcker, Wh0vt, wings, X6M9K, xqwf7, YANGZ
```

Table 2. Known Gh0st magics not investigated in this paper.

The length of the magic is by default 5 bytes, but this is not the case for all variants. In Table 1 there are magics with non-standard length – “Spidern” and “W0LFKO” – and we have seen others that were not included in this investigation, like “DrAgOn” and “QQ_124971919”.

The Spidern variant is non-standard in another way as well. It does not compress its network traffic, something most other Gh0st do. However, when looking at the code in the disassembler IDA Pro, the code relationship is clearly visible.

Fig 2 Spidern vs Gh0st comparison

Clusters and links

Clusters are composed of samples that share common traits. Usually this will be common magic tag, but this is not always the case. Sometimes clusters can form around other parameters, such as common command & control (C&C) infrastructure. Logical links between clusters occur when samples, infrastructure components or other factors exhibit traits that belong in more than one cluster. For example, a sample with a magic of "cb1st" obviously belongs in the *cb1st* cluster, but if the C&C server it connects to also accepts connections from samples using the magic "whmhl", then there is a logical link between the *cb1st* and *whmhl* clusters. The strength of such links varies, as there always are possible sources of error which are difficult to map out fully. Such uncertainties can *be to what extent is a malware variation shared or sold*, or *to what extent is command & control infrastructure hired out or shared*.

Because of these uncertainties, we will only point out where links do exist, without offering hard conclusions.

Overview plot – with Gh0st

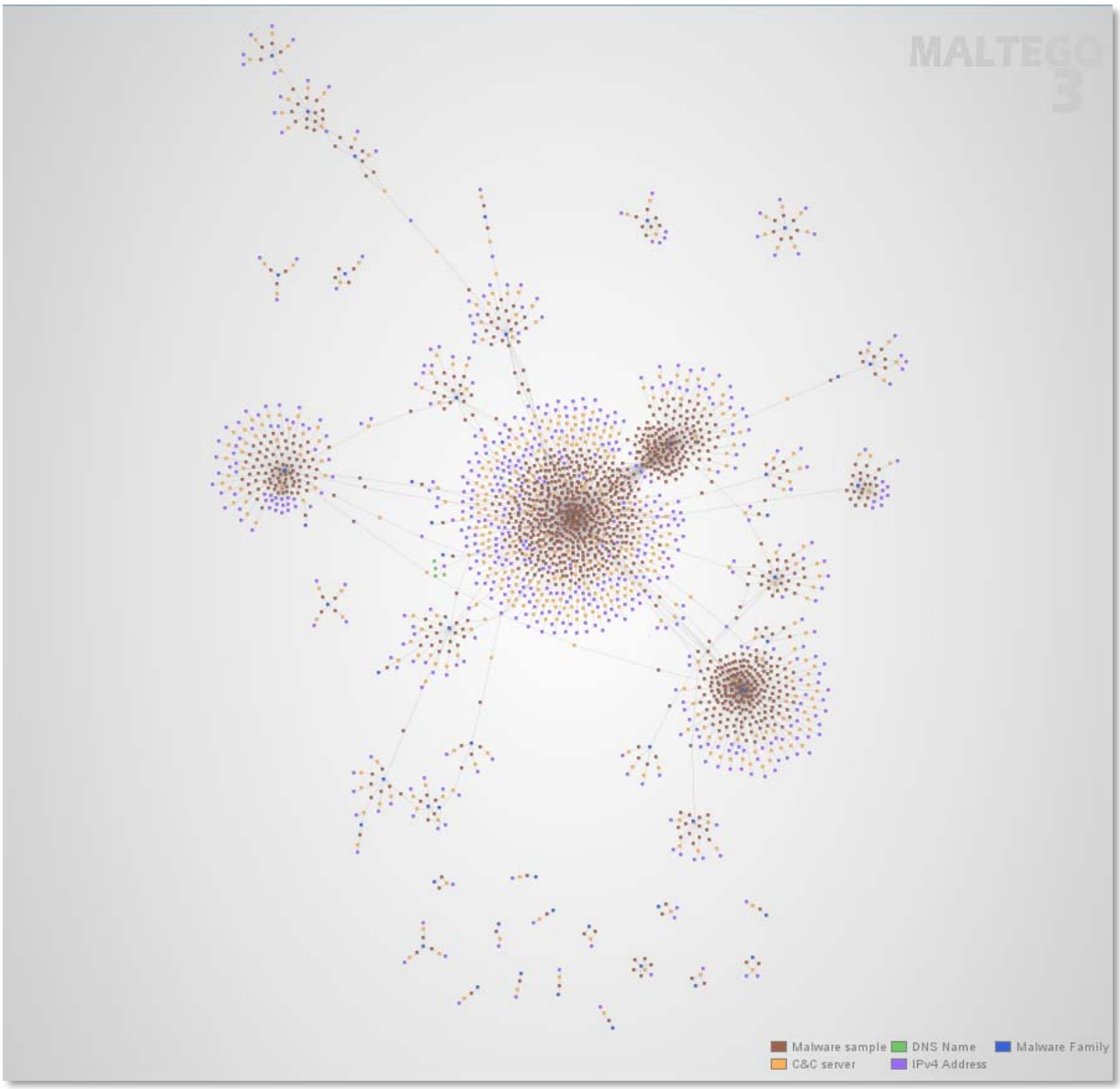


Fig 3 Overview with the Gh0st cluster

This mosquito swarm consists of trojan files, interconnected primarily by their magic tag, but also by whatever other factor shared with other samples – which C&C server they dial back to, and sometimes which IP address this resolves to. The large kludge in the middle is the default Gh0st group totaling 522 nodes.

A better overview is perhaps gained by removing the "Gh0st" cluster from the graph, as it is the default configuration and not usable for connecting clusters. Doing so results in a smaller set of more distinct clusters, where the connections are more visible.

Overview plot – without Gh0st

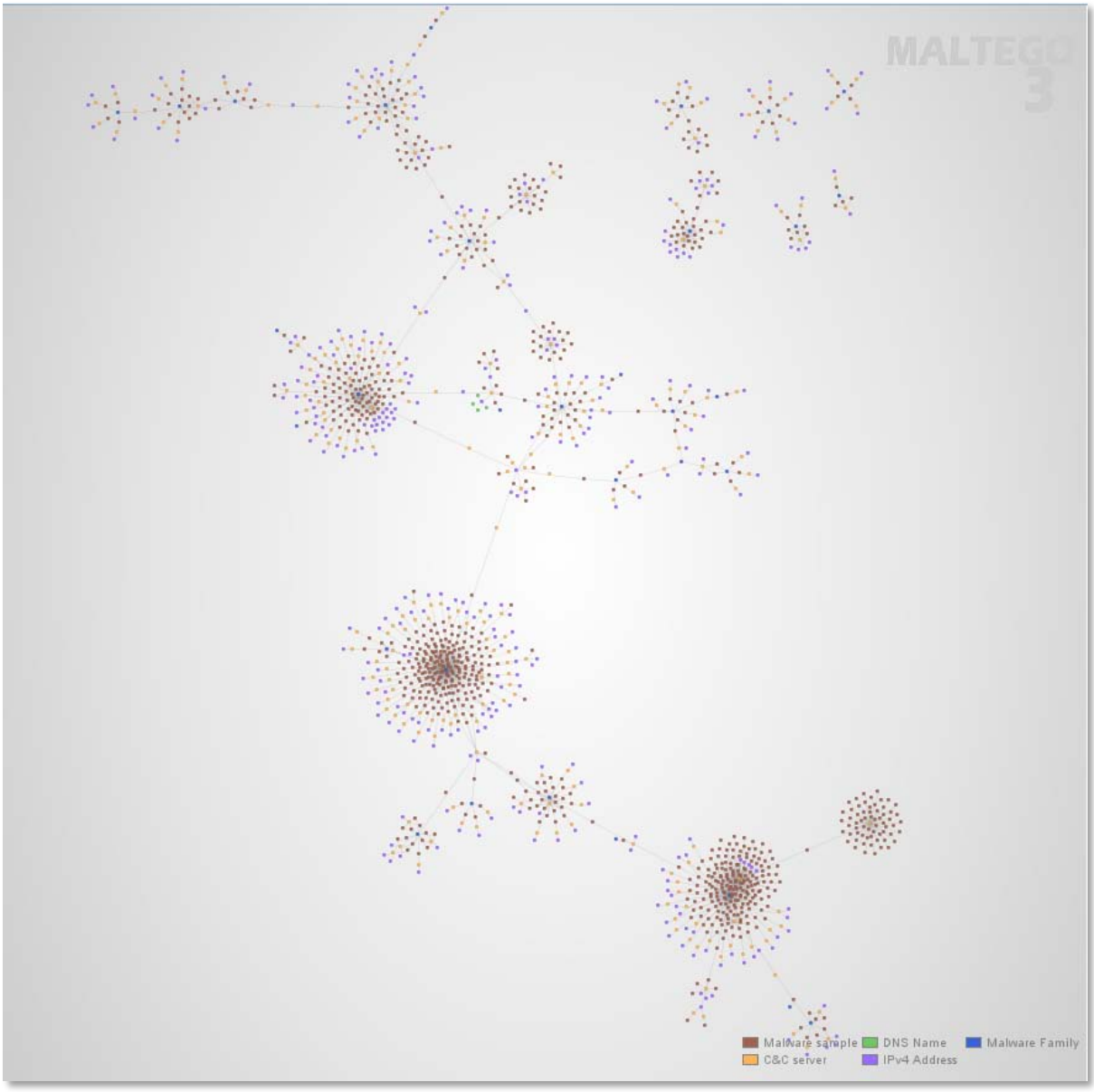
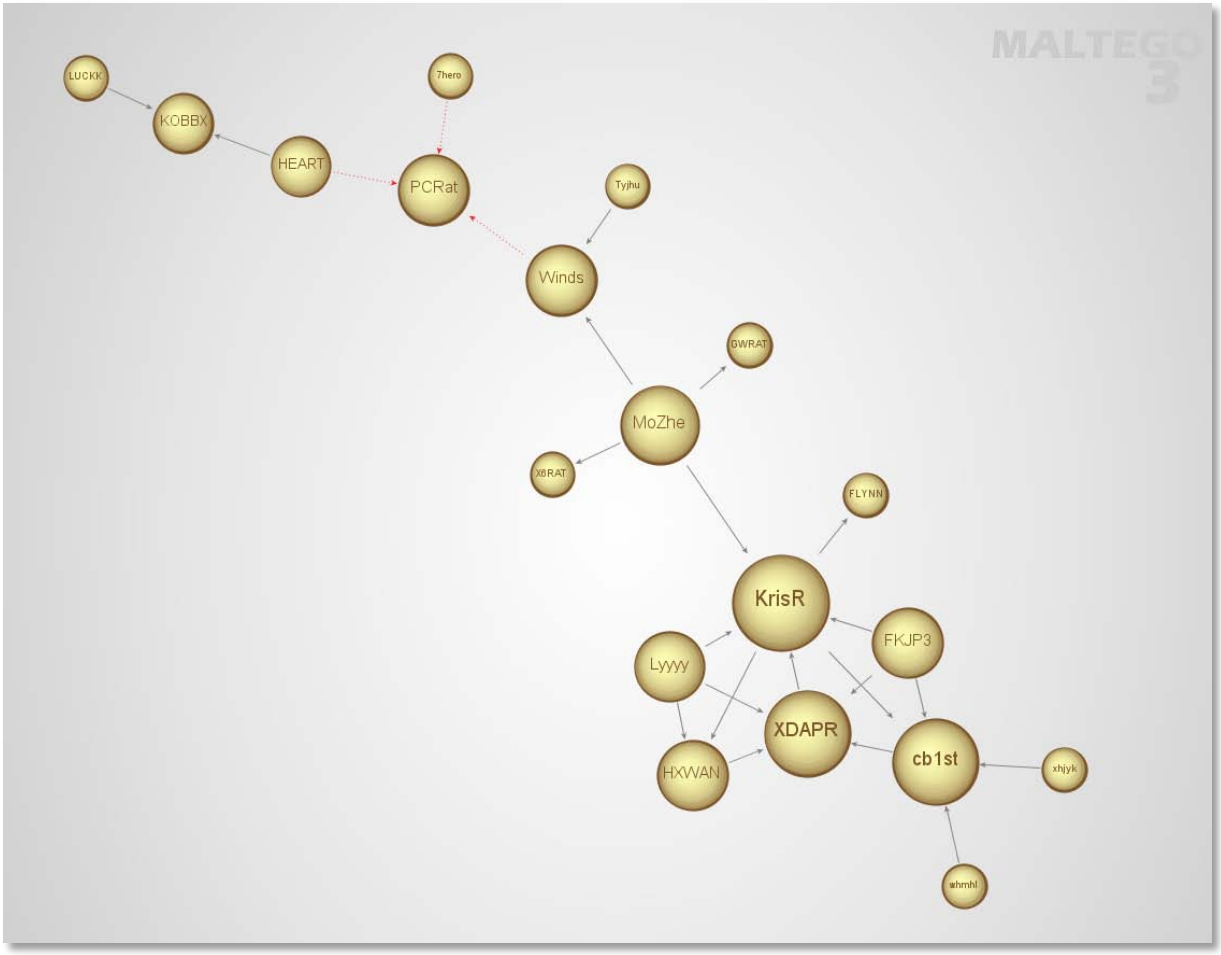


Fig 4 Overview without the Gh0st cluster

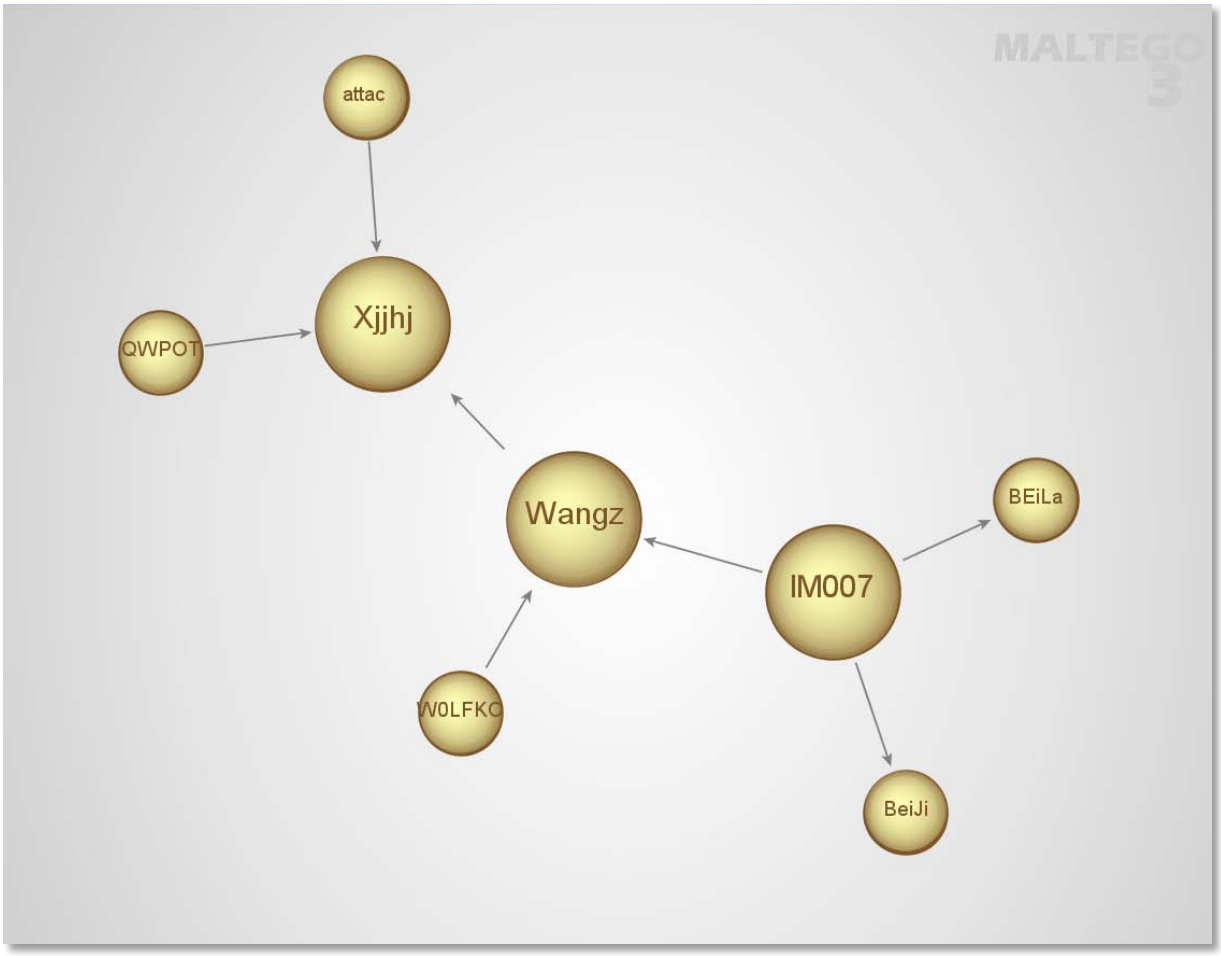
The clusters that link together form clusters of clusters. Stealing unashamedly from astronomy, let's call these superclusters. How such superclusters are linked together is detailed in the chapters that cover individual clusters later in this paper.

Supercluster one



This collection of linked clusters contain some of the most populous in the whole set. They are linked through the usage of the same C&C servers, through the same malware, and through the same observed network traffic. The links running through the PCRat cluster are dotted red as they are presumably weaker than the others.

Supercluster two

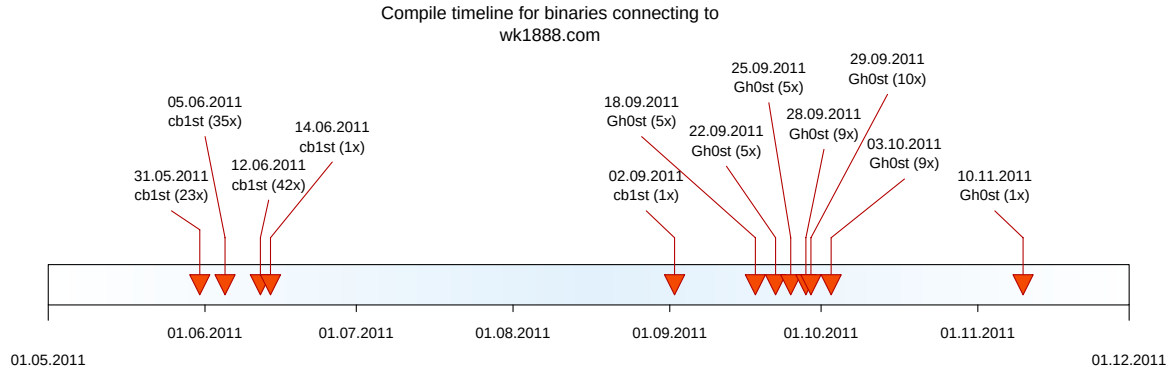


Supercluster two contains some small and medium size nodes, and indeed one cluster, IM007, that has no registered samples in this sample set. Some samples from these clusters have exhibited behavior indicating that they have been used in connection with game account theft.

Example botnet infrastructure: wk1888.com

A large amount of samples connected to **www.wk1888.com**. This host accepted connections from at least two botnet clusters – Gh0st on port 8000, and cb1st on port 8181. We have also seen Gh0st samples attempting to connect on port 8080 without being able to establish communication.

This multi-botnet support appears usually to be related to timing. Based on the header timestamp of the trojan files, the port 8181 *cb1st* samples were predominantly created May-June 2011, while the port 8000 *Gh0st* samples were created Sept-Oct 2011.



WK1888.COM has resolved to many IP addresses over time, all belonging to Krypt Technologies [AS 35908], a US-based VPS hosting service. At the time of writing the IP is 174.139.51.150. The same WHOIS info points to the domains af0575.com and fz0575.com, both associated with earlier Gh0st Rat samples, and to the domains wt1888.com and 81266966.com.

The wk1888.com host ran at one point a webserver on port 2011 where it hosted download information and more executables to download. A sample which used this functionality was a downloader executable (md5 b6e900f8a14740aa6ad3e755dc2d14bb), which performed the transaction below:

```
GET /1.txt?abc=78823 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET4.0C; .NET4.0E)
Host: www.wk1888.com:2011
Connection: Keep-Alive

HTTP/1.1 200 OK
Content-Length: 69
Content-Type: text/plain
Last-Modified: Tue, 15 Nov 2011 12:02:04 GMT
Accept-Ranges: bytes
ETag: "d446d6638ea3cc1:276"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Wed, 16 Nov 2011 01:26:05 GMT
hxxp://www.wk1888.com:2011/1.exe
hxxp://www.wk1888.com:2011/xf80.exe
```

The 1.exe file (md5 00118d190f8a30e6dc70b394e603d155) is a Gh0st trojan of the cb1st cluster, connecting back to wk1888.com on port 8181. The xf80.exe file is a DarkShell DDOS trojan (md5 d47e37178c0d5b8780b97ce4e7c0e06b).

Similar functionality was seen on wt1888.com (e.g. 68fdd8adf91308cf35a2e86b15ce6cdd) (2), and on 81266966.com. The latter hosted downloader and DDOS trojans that connected back to wk1888.com (3)

Attribution wk1888.com

The WHOIS information for wk1888.com is as follows:

```
WK1888.COM

Administrative Contact:
      meng, meng  1377887494@qq.com
      east china jiaotong university
      nanchang, jiangxi 330013
      China
```

The same registration information is used for the domains 81266966.COM, WT1888.COM, FZ0575.COM and AF0575.COM.

Googling the email address "1377887494@qq.com" shows that it is also used to register the domain "boyul.com", but with different address/phone information.

```
BOYUL.COM

Administrative Contact:
      wenyan zhong  1377887494@qq.com
      telephone: +86.051052478530
      fax      : +86.051052478531
      jiangsu wuxi hehuali wuxi jiangsu 214000
      CN
```

Boyul.com resolves at the time of writing to the IP 174.139.63.18, which also belongs to Krypt Technologies and has historically even been resolved to by wk1888.com.

The data (phone/address) used to register boyul.com match literally thousands of other domain registrations: HON168.COM, 1585GB.COM, ZJHD518.COM, 17173CGW.COM etc.

The QQ address 1377887494 is used in several advertisements on the hacking forum my3800.com (Central China Honker Security):

出售免杀GH0ST
每天赠送50**只肉**鸡娱乐超低价200**元一个月另出租小型肉**鸡包天包月位置联系
QQ:1377887494

Translation:
"Selling undetected GH0ST kits. A package of 50 zombie machines (chicken) comes included, for 200 yuan (ca 35 USD) a month. Rent zombie machines pr day or pr month, contact me".

The QQ number is also found on the forum beishan.info (4), where the poster complains about problems with the registration of the domain www.sock8.com, which he claims he has bought from a registered seller on *taobao.com.* Taobao is the Chinese version of eBay.

This post was made May 27th 2011. The WHOIS info for the sock8.com domain shows that May 19th it was apparently reclaimed by Netfirms and returned to a parking IP. Before this, the domain was registered by one “bingxian feng”:

```
Administrative Info:
   bingxian feng
   bingxian feng
   na
   jiangmen, NA 529700
   China
   Phone: +1.102251166
   Fax..:
   Email: a916196832@yahoo.com
   Last modified: 2011-04-11 11:47:43 GMT
```

In the period from the domain was registered by Bingxian Feng April 11th to its apparent seizure in May a number of Ghost trojans surfaced which connected to the sock8 domain. These had an apparent compile date April 12th and 13th.

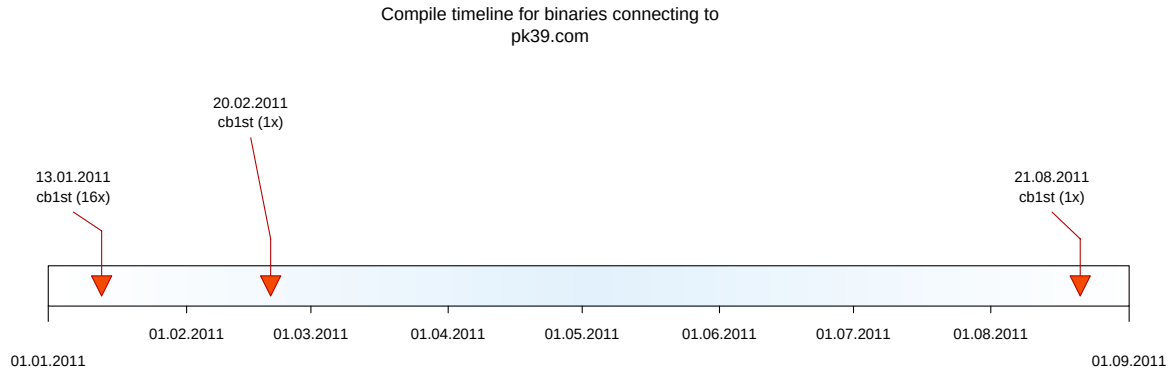
Googling for Feng’s email address in the WHOIS shows that it is used for registering literally hundreds of domains. Not only that, but it turns out that this player is well known domestically in China (5), where this person allegedly has been involved in pornography, mobile phone scams, game theft, and phishing attacks against among others *People’s bank of China.*

There are several cyberpolice departments (also known as "Net Cop") in China, organized by regions.

Example botnet infrastructure: pk39.com

This domain is the second of the two main hubs controlling the cb1st cluster. As previously mentioned ddos.pk39.com also operates C&C for the whmhl cluster, and the host down.pk39.com has acted as download server for other malware, typically DDOS trojans of various kinds.

The Gh0st trojans dialing home to www.pk39.com were with few exceptions created Jan 13th 2011.



Attribution pk39.com

Its WHOIS information is as follows:

```
PK39.COM

Administrative Contact:
  Name            : zheng xuming
  Organization    : zheng xuming
  Address         : leqing huayuan lukou
  City            : xianggangtebiexingzhengqu
  Province/State  : xianggangtebiexingzhengqu
  Country         : xianggangtebiexingzhengqu
  Email           : 924539333@qq.com
```

The email 924539333@qq.com shows up a number of places through Google. One interesting reference is found on the site www.kissqc.com, which just says:

This is not the only defacement attributable to CǒCǒ – his name is found several places in similar fashion. He also appears to use another handle frequently associated with hacking.

These handles appear to match the online profile of a male in his mid-twenties, living in Changzhou in the Jiangsu province of China. He appears to be involved in many other projects, from Android development to network security tools. The word “Ghost” is ironically used in a lot of his projects.

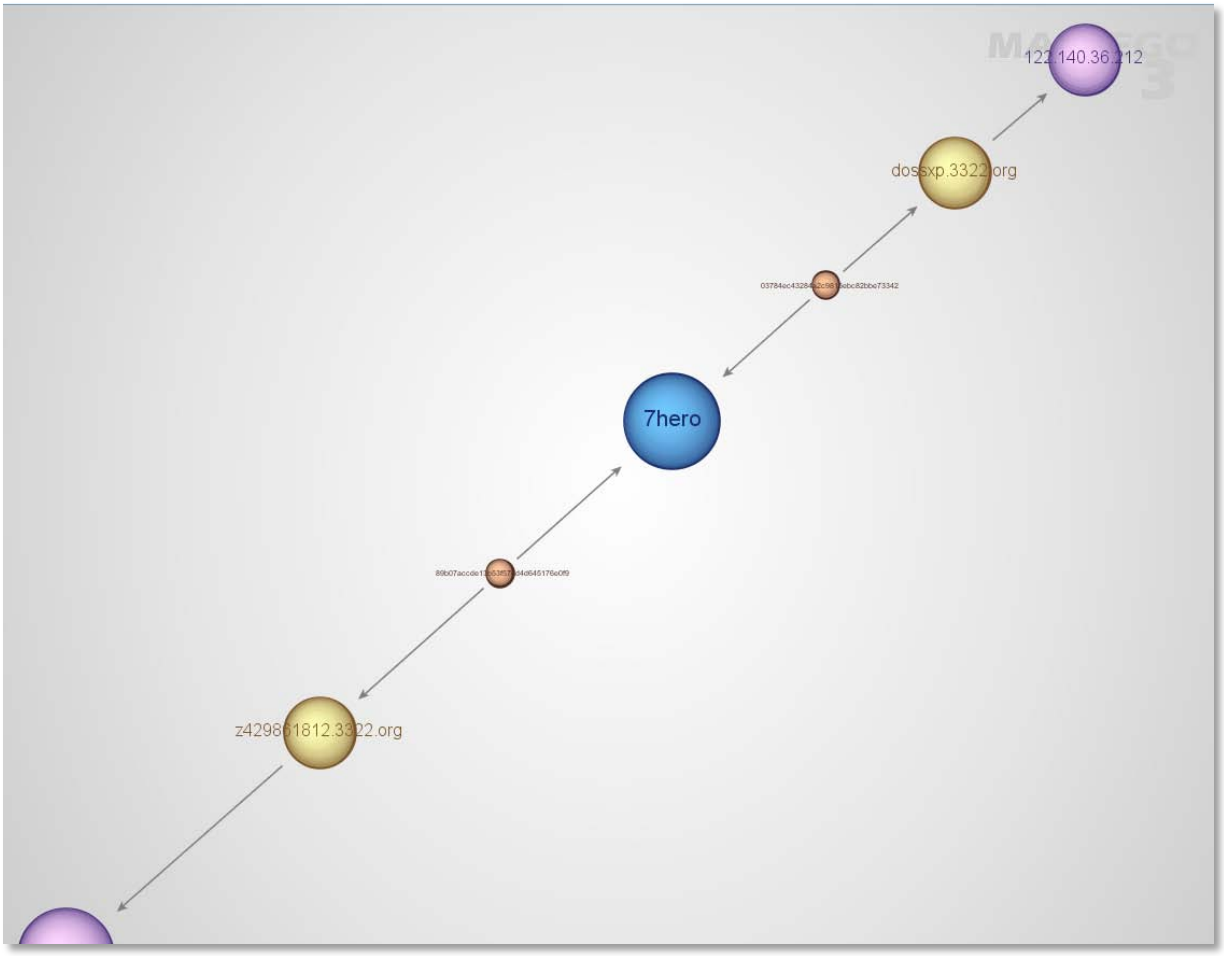
Individual clusters

What follows is a listing and description of the individual botnet clusters. This is fairly lengthy, so feel free to skip to ***Conclusion*** towards the end of the document.

Some explanation to the individual cluster graphs to come:

Brown nodes are samples
Blue nodes are malware families (i.e. usually Gh0st variants)
Yellow nodes are C&C servers (hardcoded IP or DNS name)
Purple nodes are resolved IP addresses

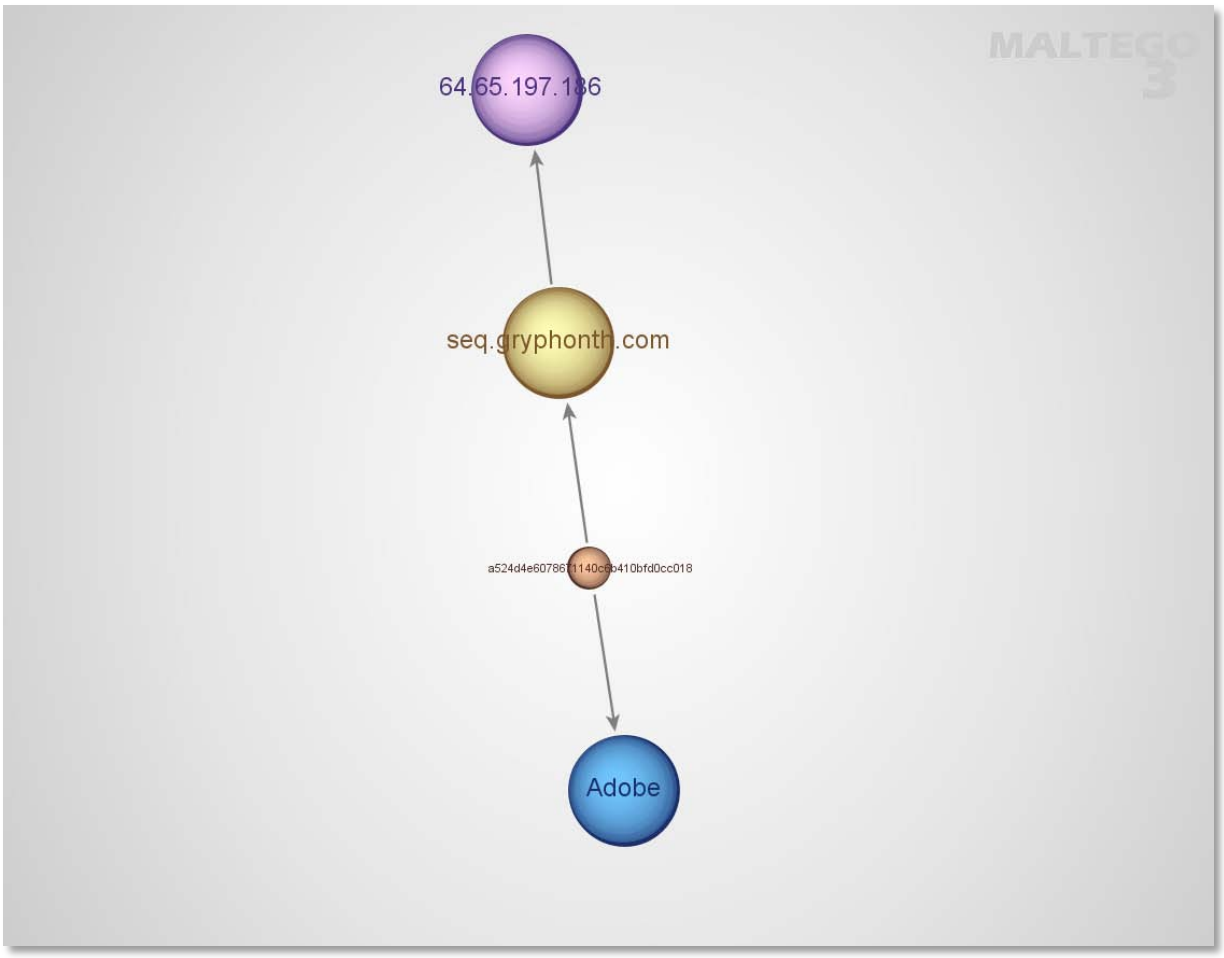
Cluster: 7hero



The 7hero cluster has two samples in the set. It is linked with the PCRat cluster through the shared IP address 61.147.123.11 between the PCRat server at 429861812.3322.org and the 7hero C&C server at z429861812.3322.org. This could have been a coincidence - however, they both also connected at port 4928, something that only these two samples in the whole test set did.

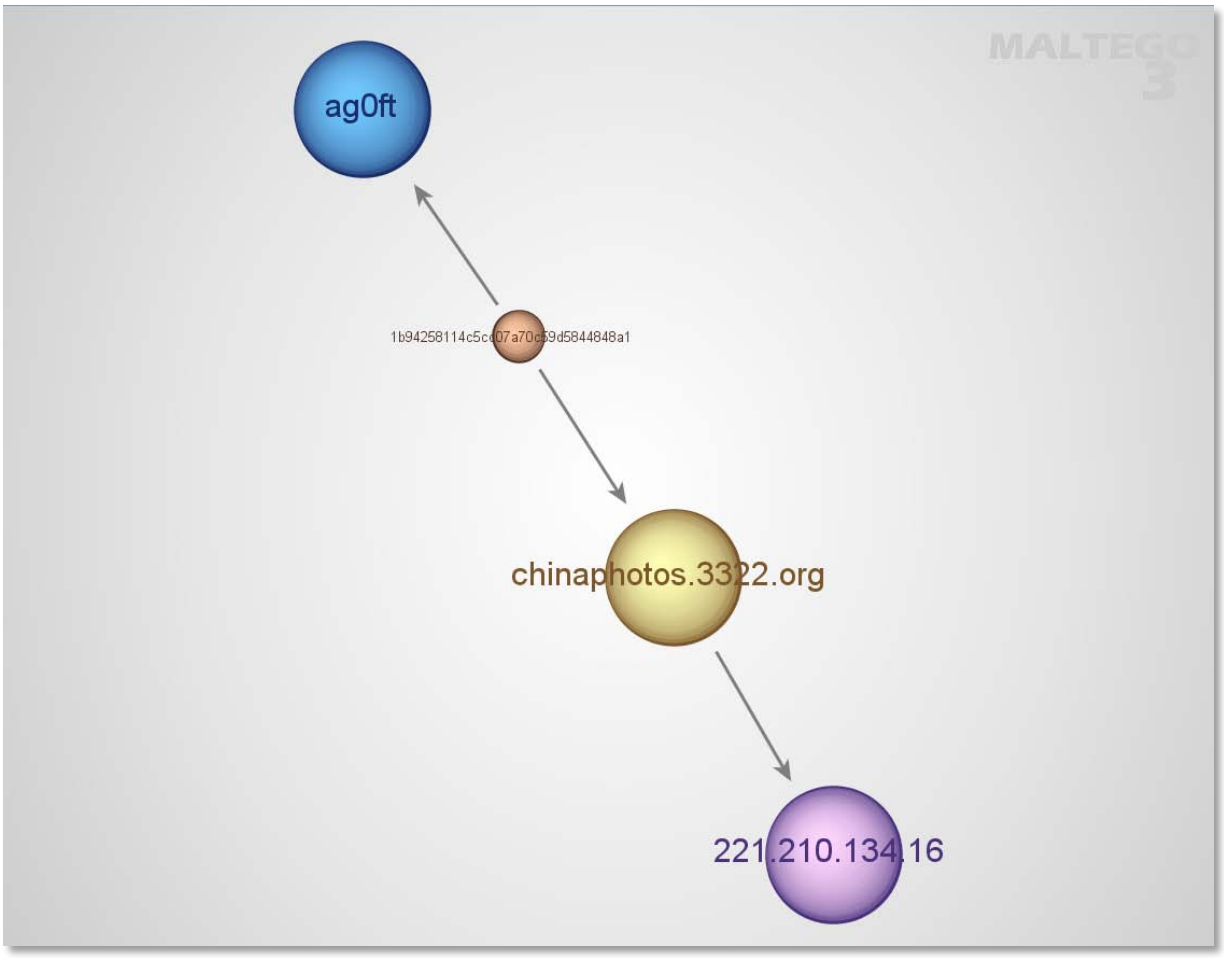
z429861812.3322.org is also used as C&C for samples in the Gh0st cluster.

Cluster: Adobe



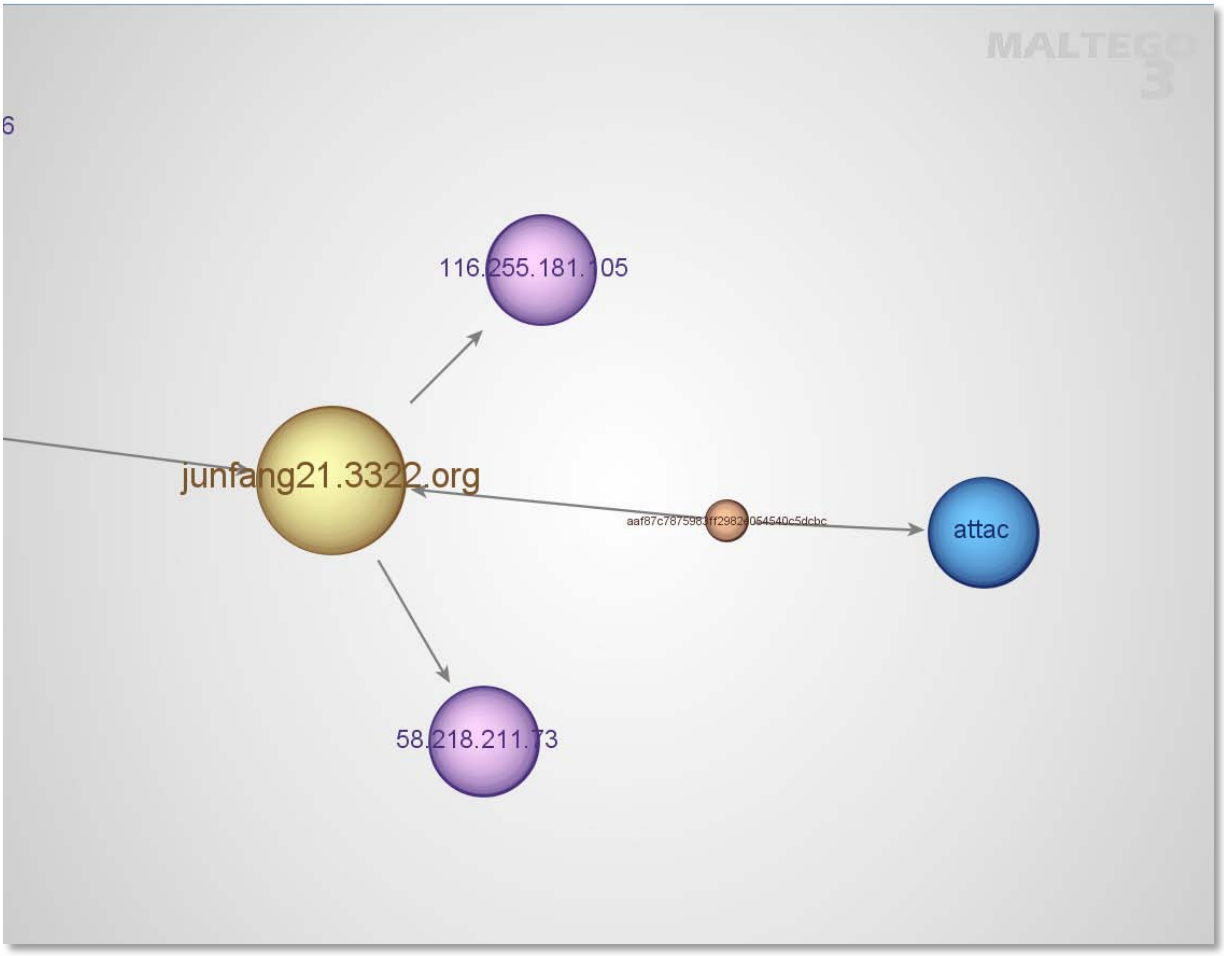
The Adobe cluster contains one sample, and appears not linked with other clusters.

Cluster: ag0ft



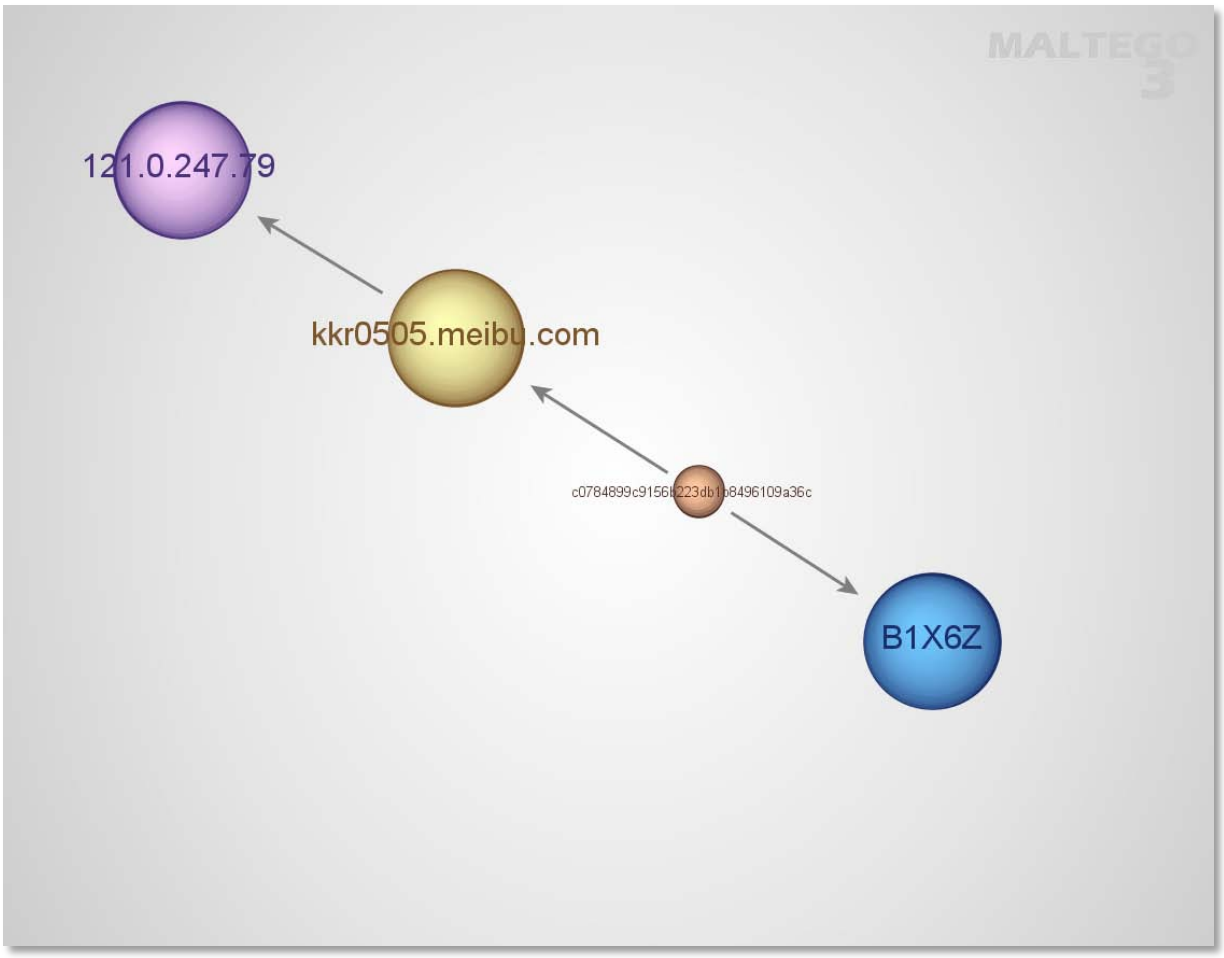
The ag0ft cluster contains one sample, and appears not linked with other clusters.

Cluster: attac



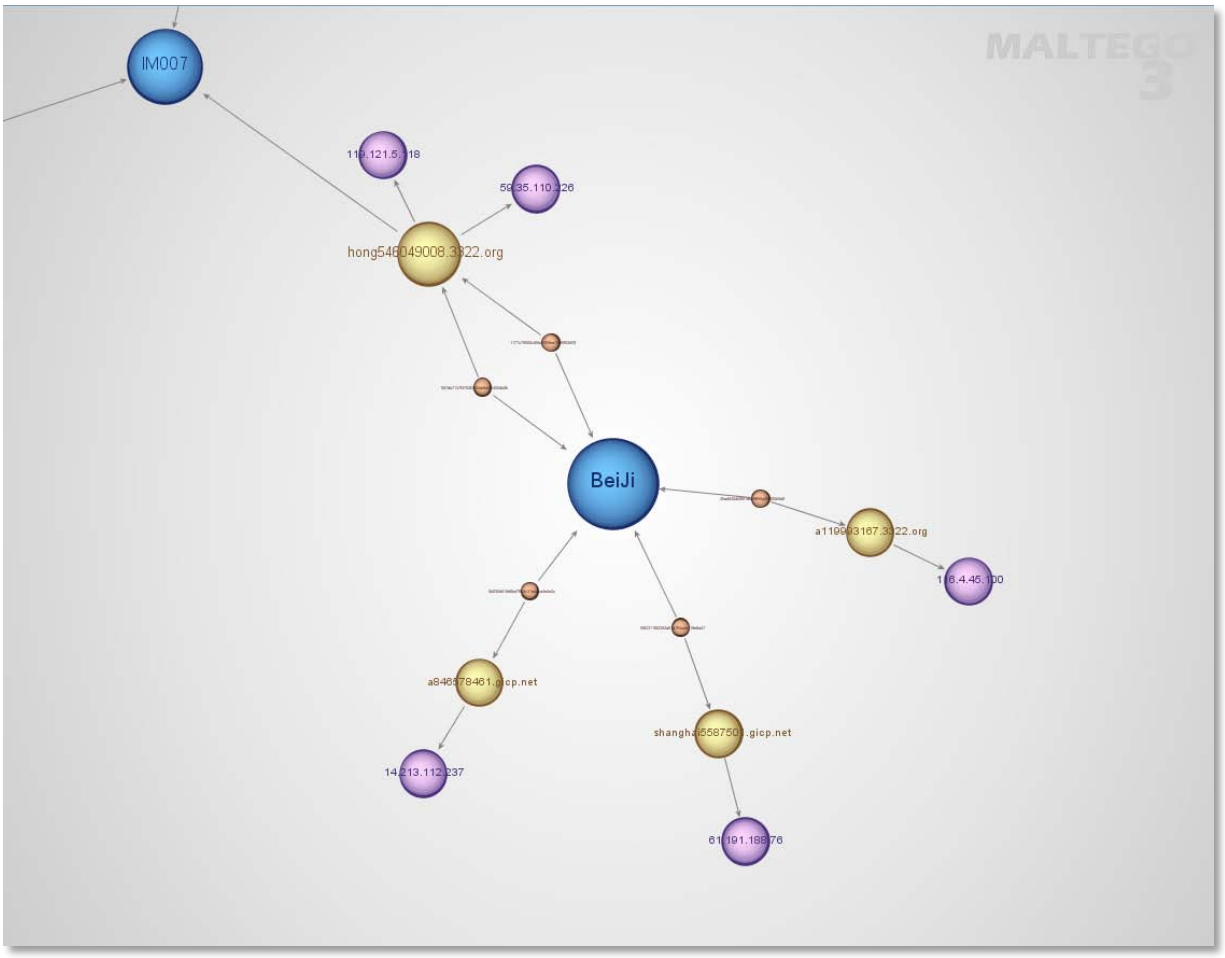
The attac cluster contains one sample, and is linked with the Xjjhj cluster through shared C&C at junfang21.3322.org. This C&C server has also served as C&C for Netbot Attacker DDOS bots.

Cluster: B1X6Z



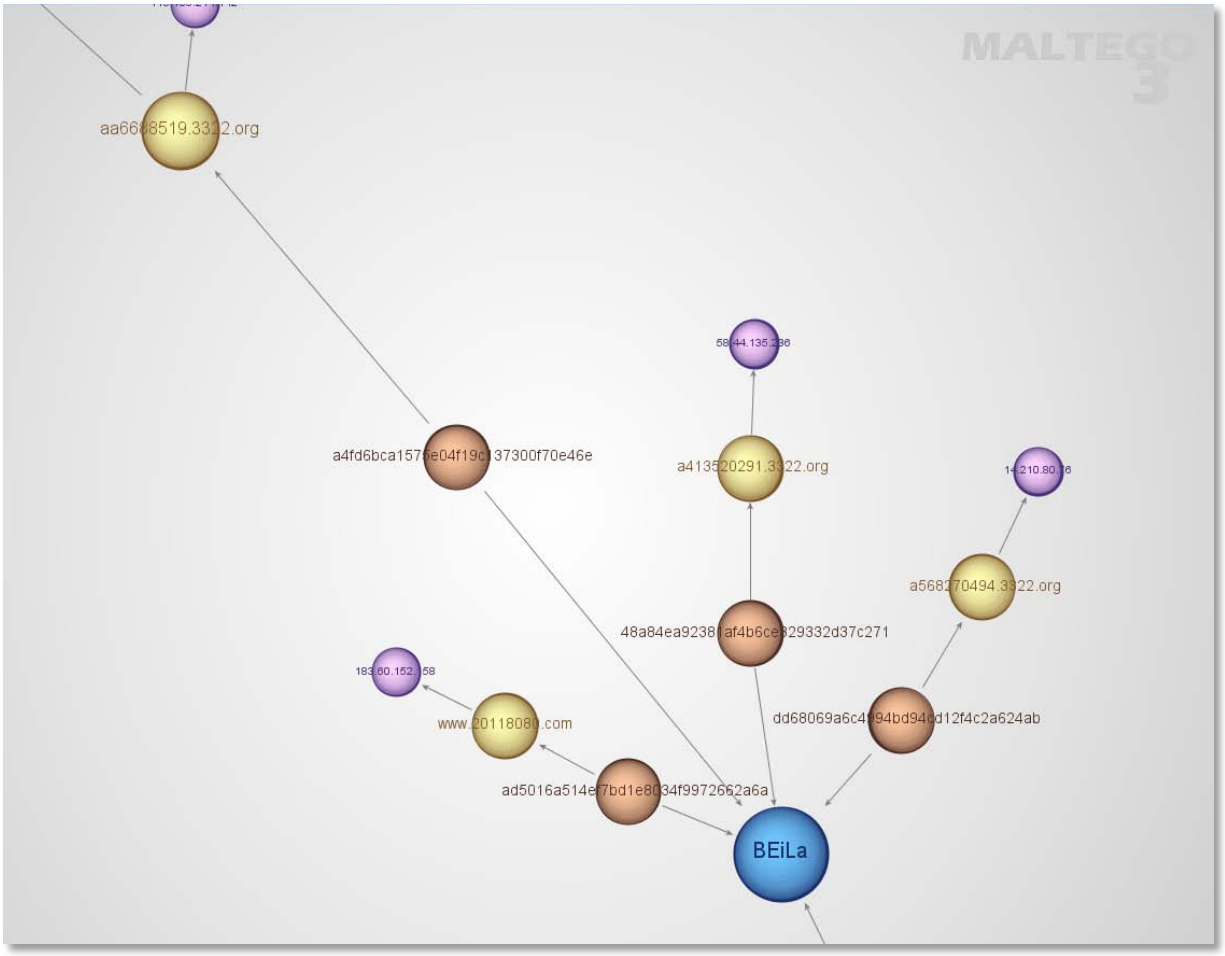
The B1X6Z cluster contains one sample, and appears not linked with other clusters.

Cluster: BeiJi



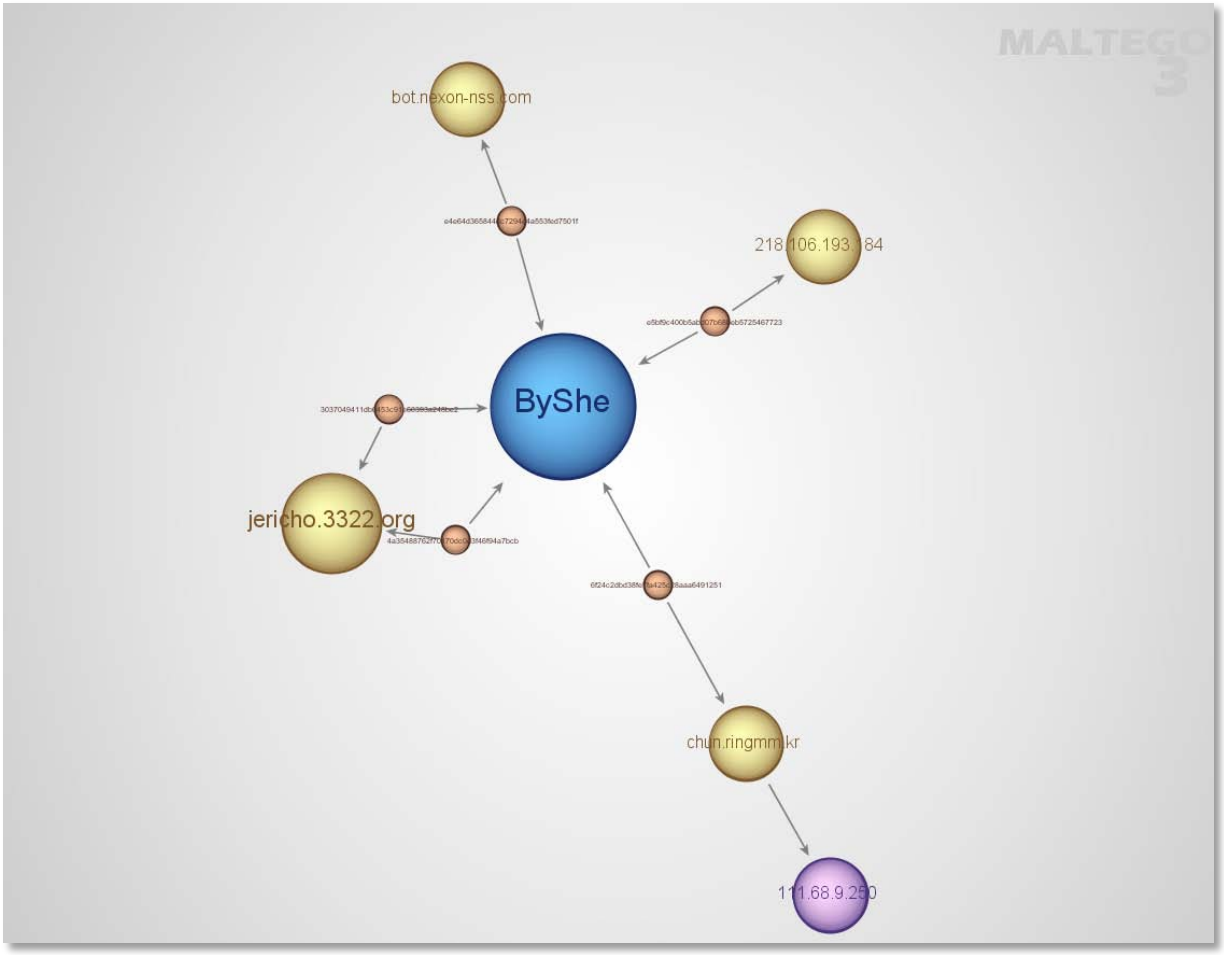
The BeiJi cluster contains five samples. Two of these samples connect to hong546049008.3322.org, a server which is shared with the IM007 cluster.

Cluster: BEiLa



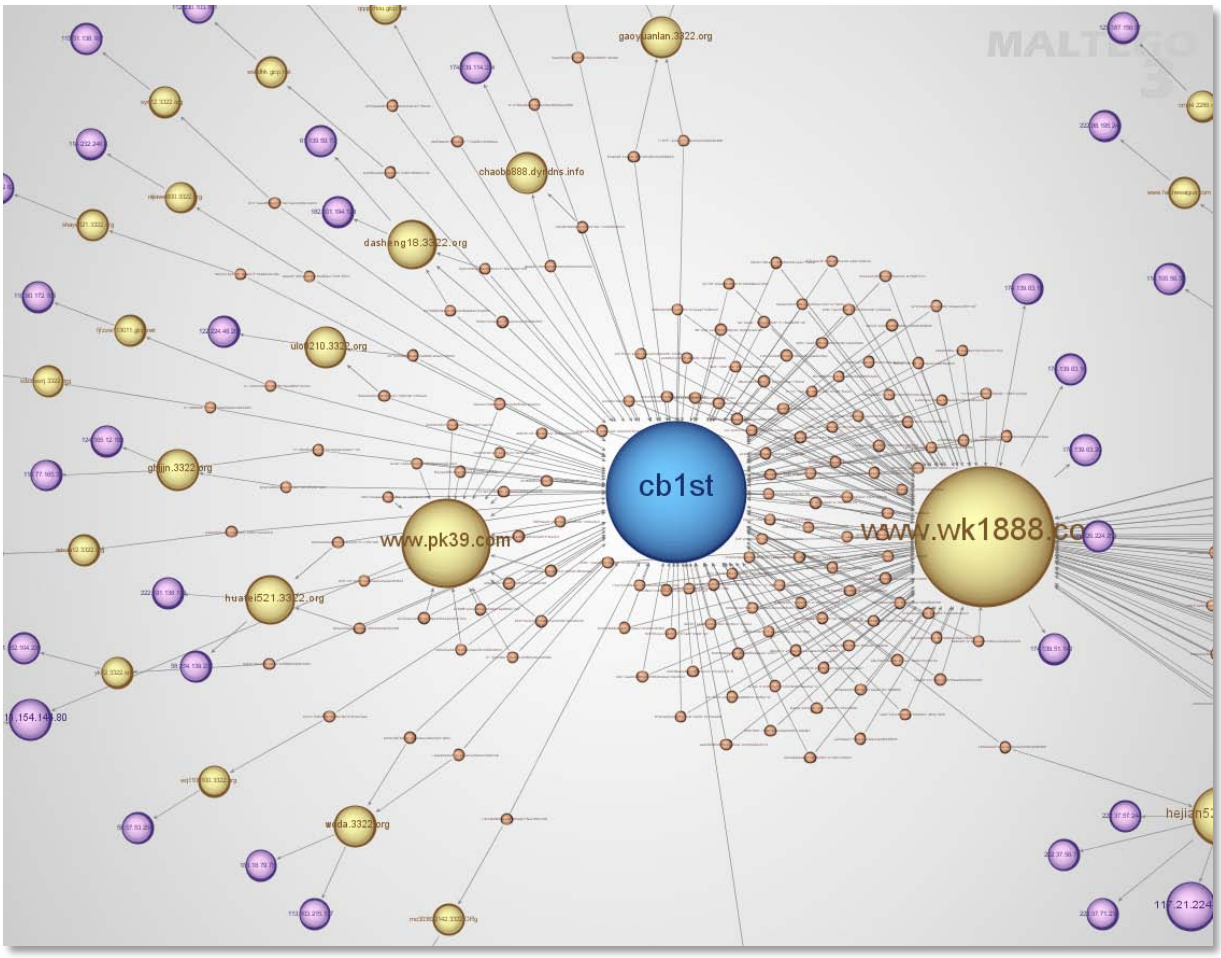
This cluster contains 5 samples and is linked with the IM007 cluster through observed traffic from the C&C server aa6688519.3322.org.

Cluster: ByShe



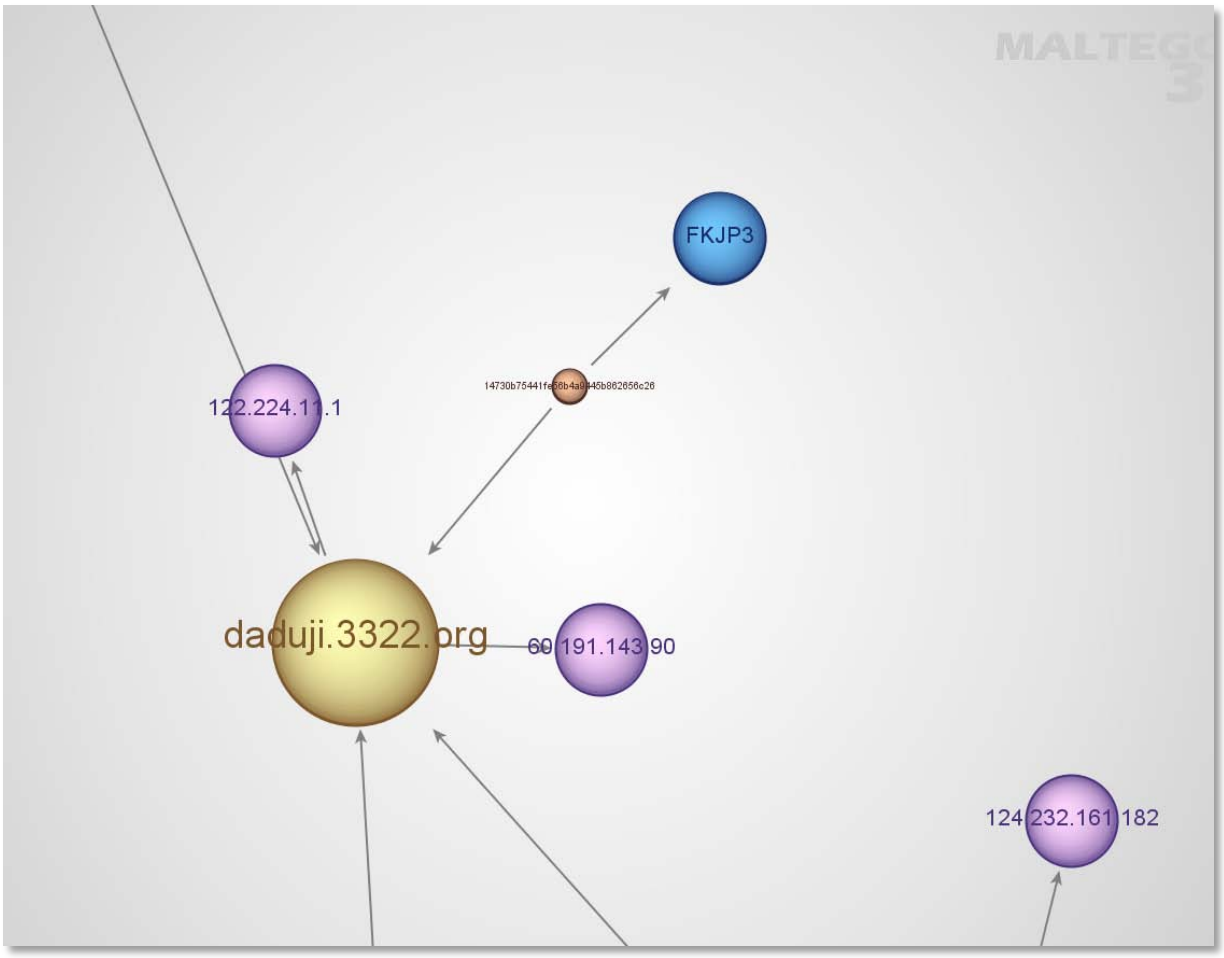
The ByShe cluster is interesting, as it has been documented used in targeted attacks against Tibetan groups (6) and also connected with the Nitro attacks (7). Five samples exist in this cluster, though no other clusters links with it.

Cluster: cb1st



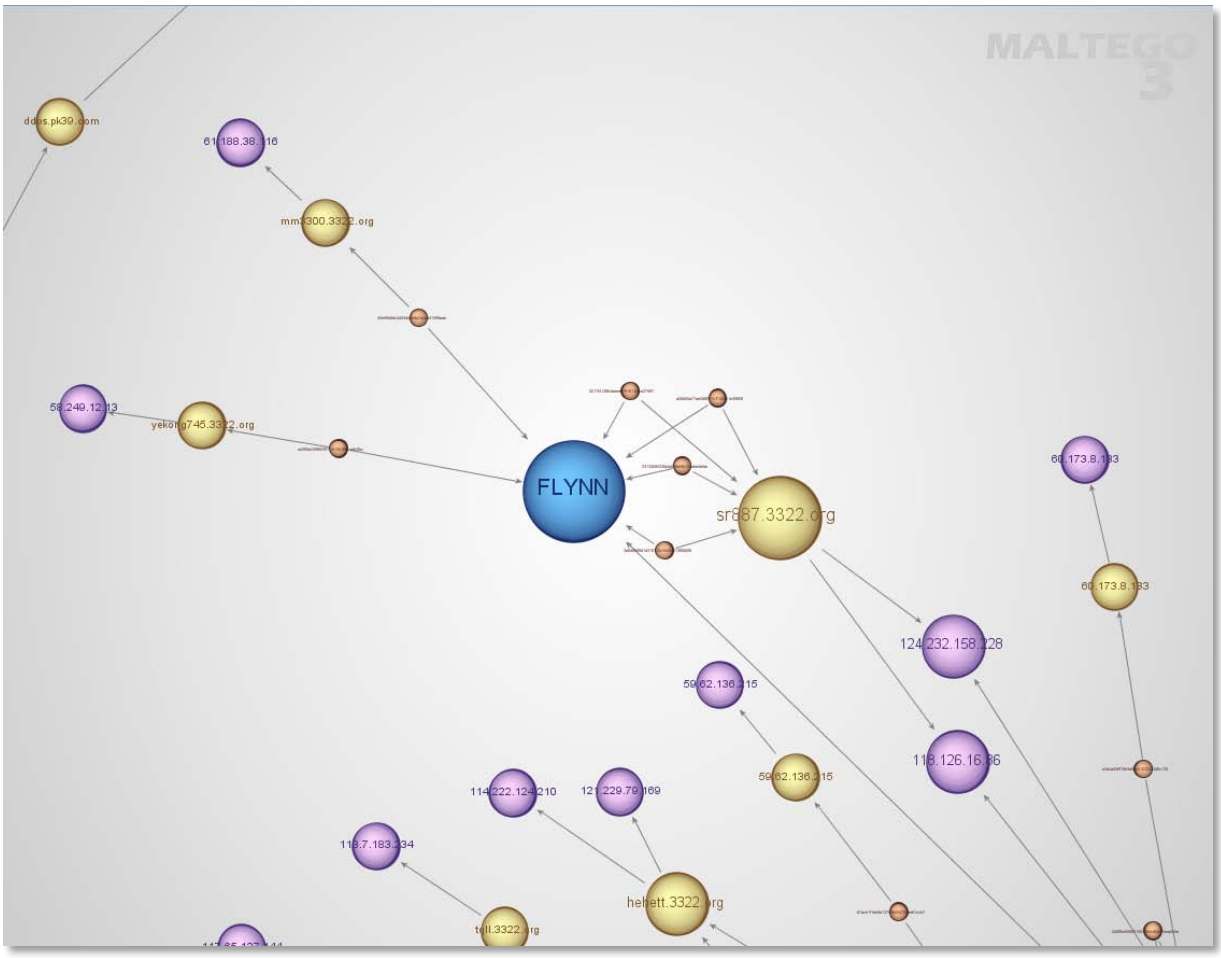
The cb1st cluster is one of the larger, with 154 samples. The major C&C's here are www.wk1888.com and www.pk39.com. The wk1888.com host also acts as C&C for many samples in the Gh0st cluster. cb1st is linked with the KrisR, XDAPR and FKJP3 clusters through the C&C at daduji.3322.org. The www.pk39.com host links cb1st with the whmhl cluster through observed traffic (see whmhl).

Cluster: FKJP3



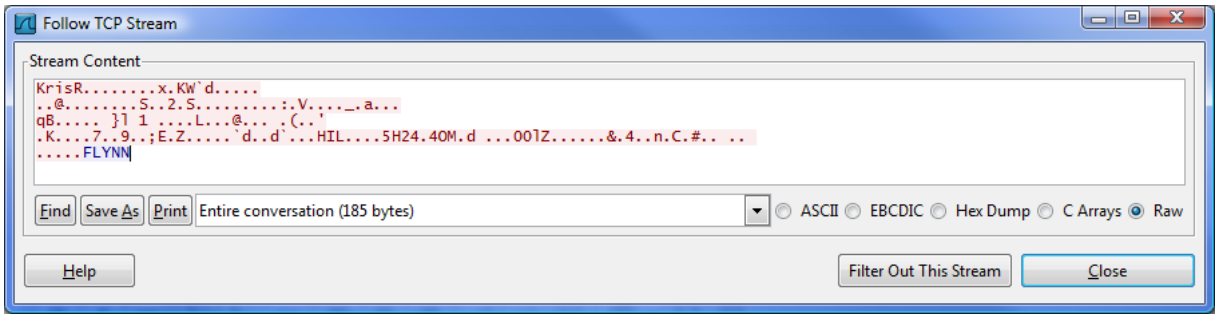
There is only one sample in this cluster. Through its C&C at daduji.3322.org it links to KrisR, XDAPR and cb1st clusters.

Cluster: FLYNN

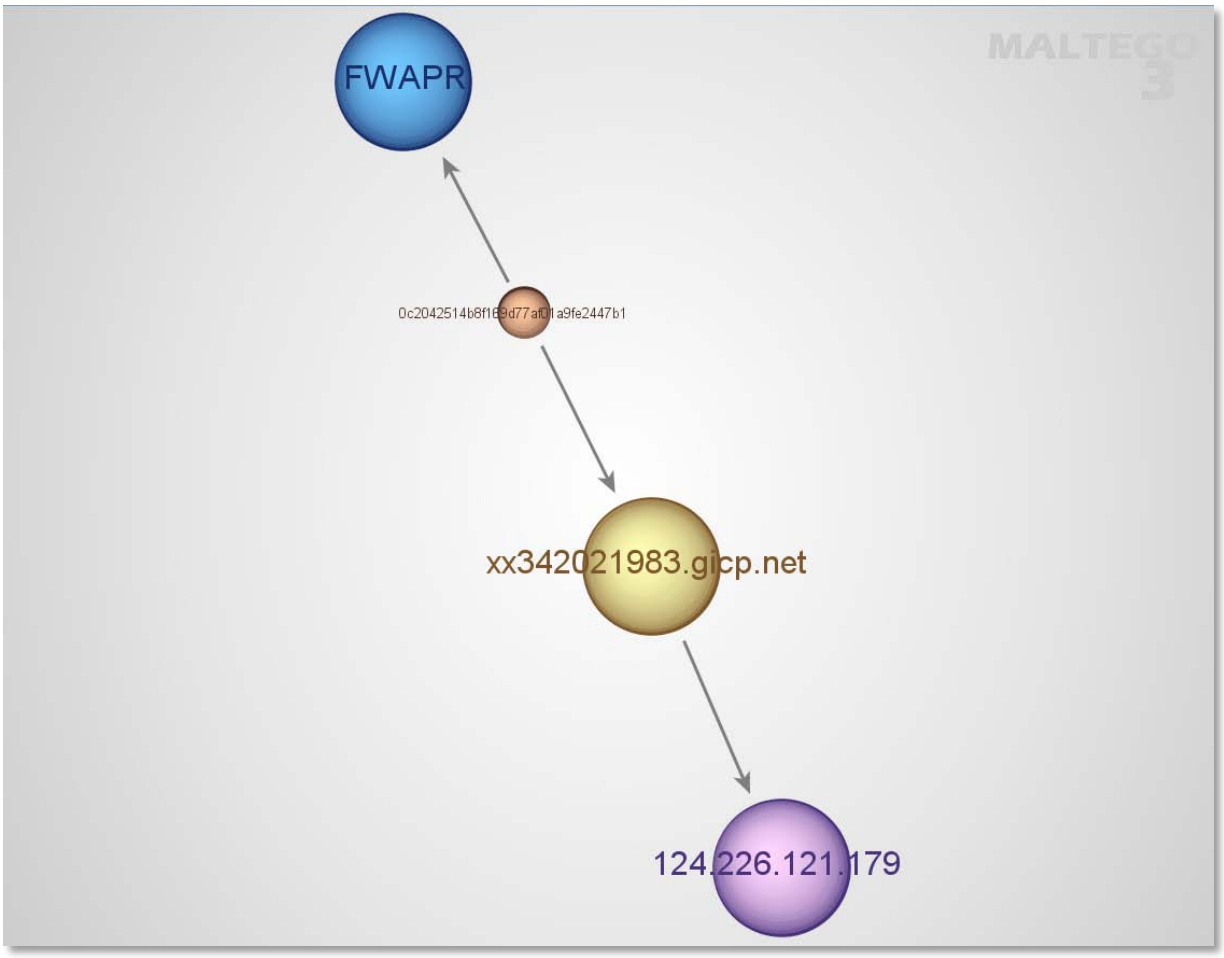


The FLYNN cluster consists of 6 samples. It is linked with the KrisR cluster because of common C&C at 118.126.16.86 and observed traffic returning FLYNN to a KrisR sample.

MD5	Host	IP	Port	Outgoing	Incoming
919a4d03cc9dde709b0f2b05a082b179	haidishijie.3322.org	118.126.16.86	8888	KrisR	Gh0st
5217f4148fcfabee2791611cfce27997	sr887.3322.org	118.126.16.86	6666	FLYNN	FLYNN
a28d90a77ae2d8977c31329b1e396f2f	sr887.3322.org	118.126.16.86	6666	FLYNN	FLYNN
3db213a3f5df462c8bb6cf896af63d28	haidishijie.3322.org	118.126.16.86	6666	KrisR	FLYNN
500f7f5f27ee2e4652204313dc2fcb91	haidishijie.3322.org	118.126.16.86	8888	KrisR	Gh0st

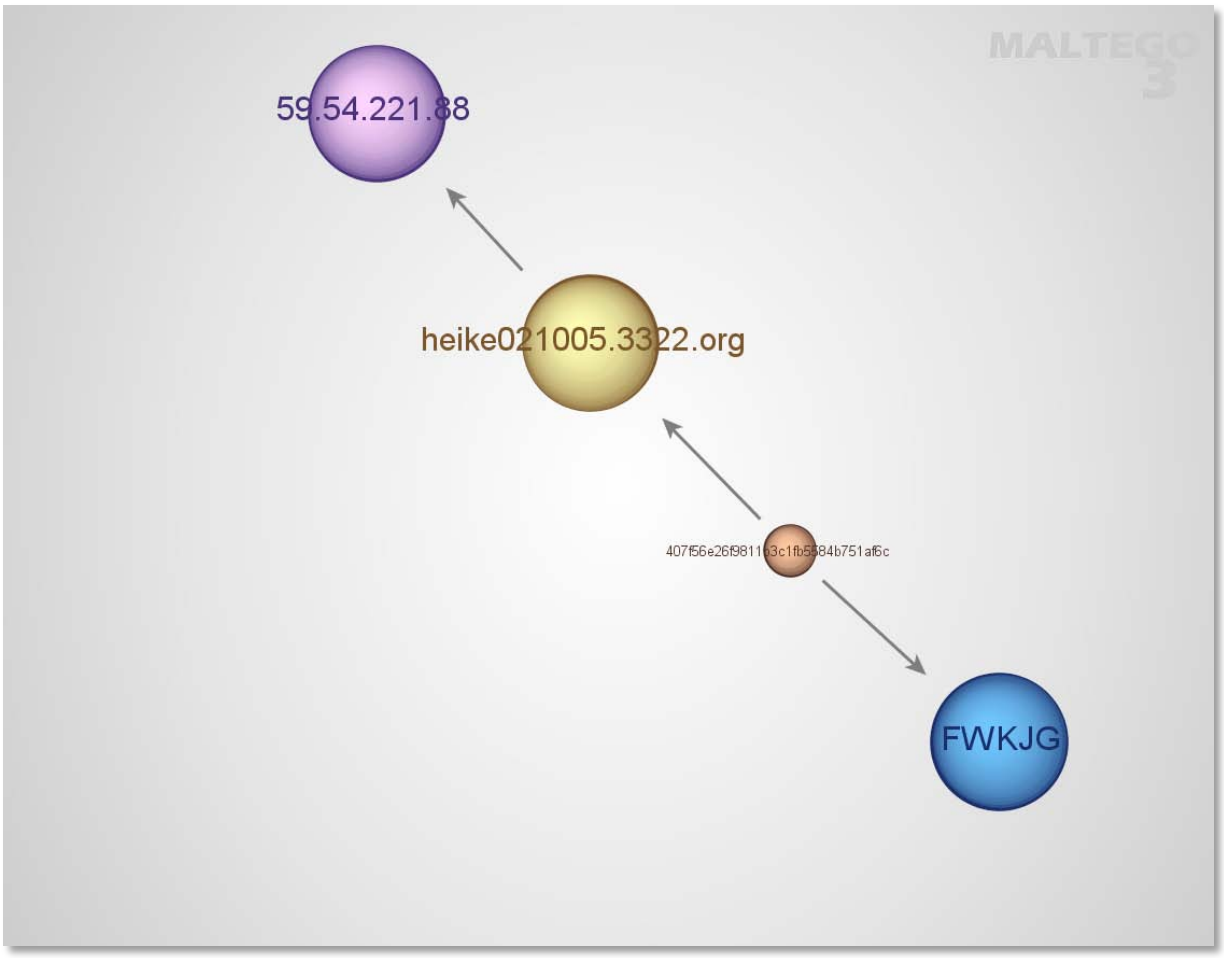


Cluster: FWAPR



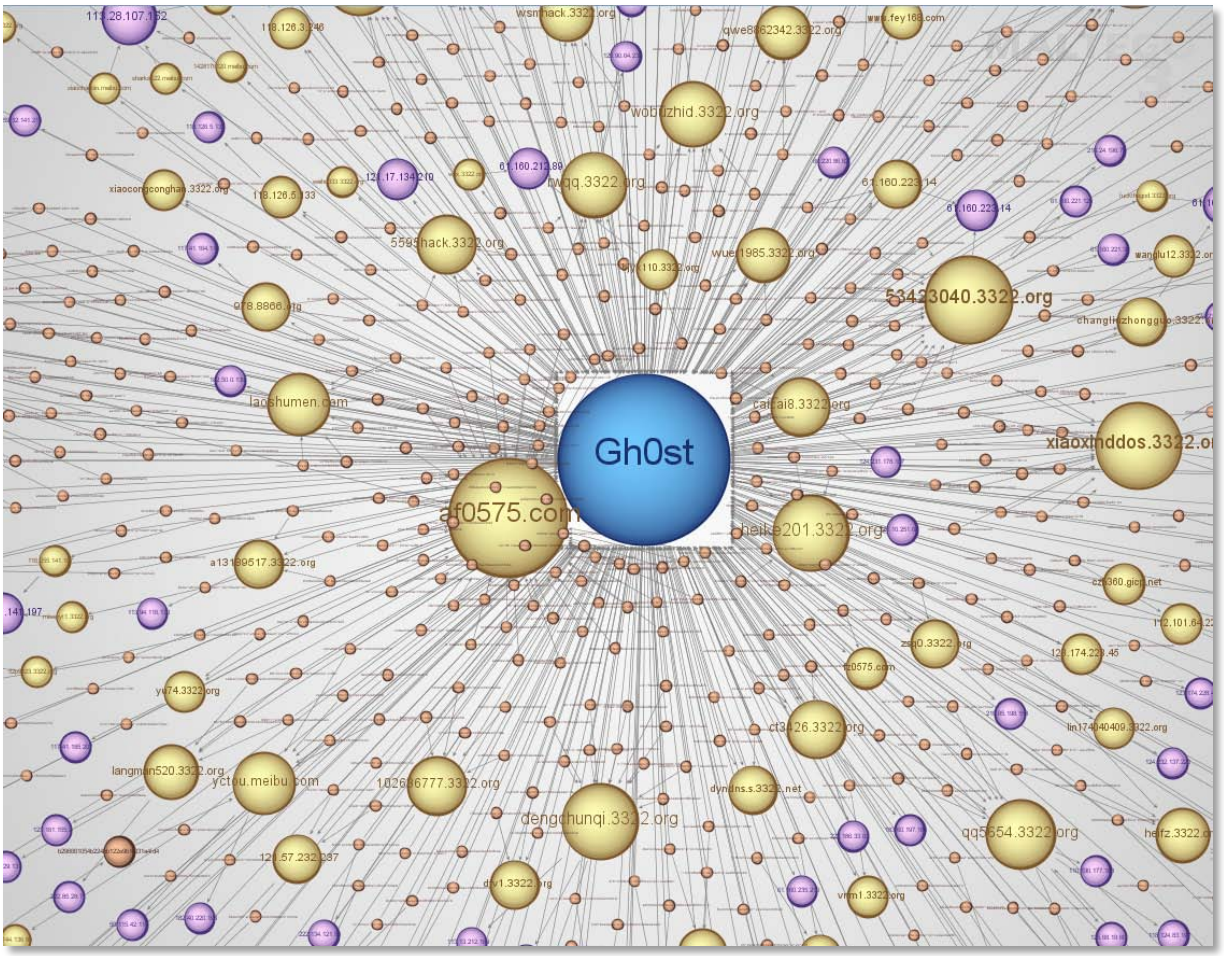
The FWAPR cluster contains one sample, and appears not linked with other clusters.

Cluster: FWKJG



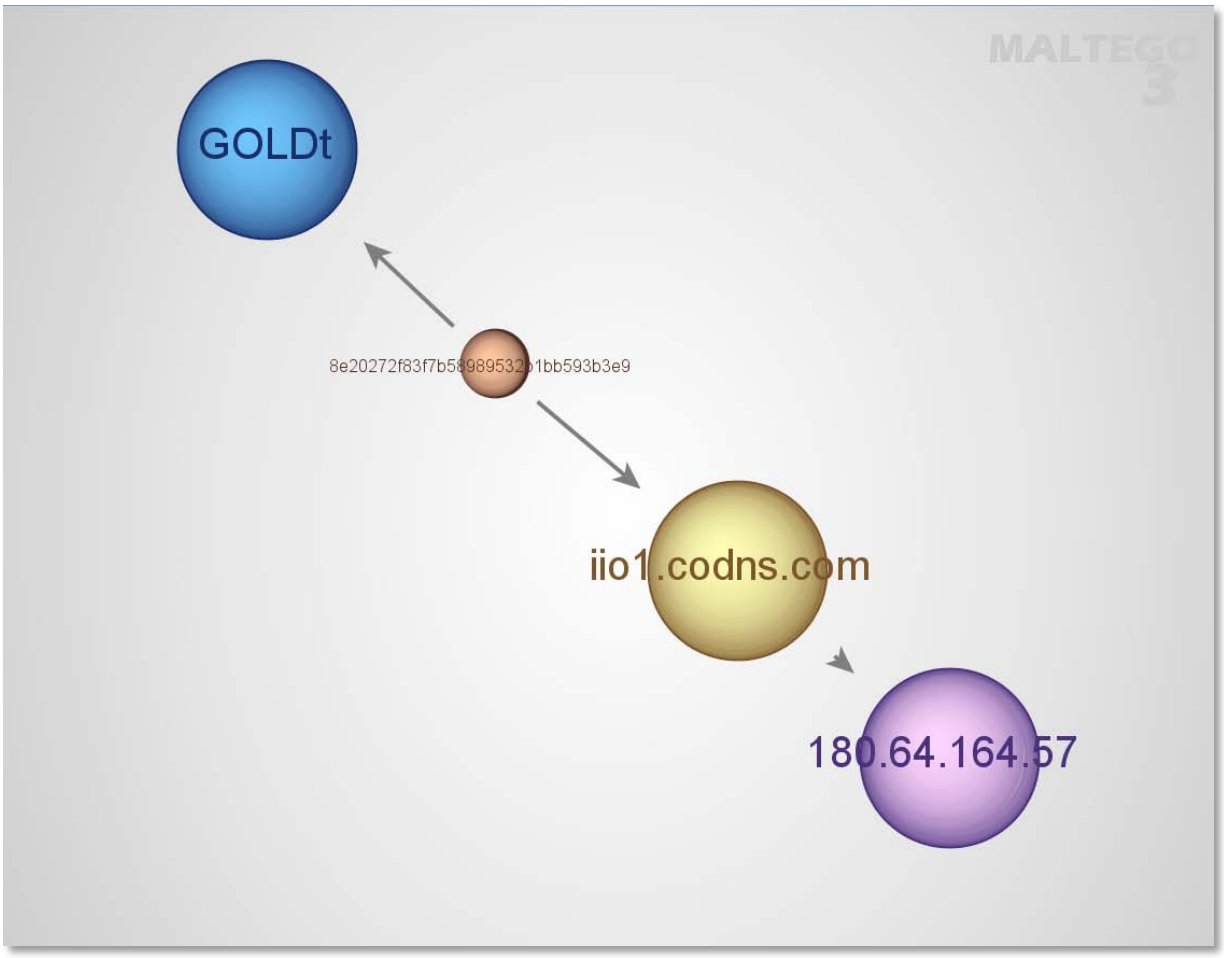
The FWKJG cluster contains one sample, and appears not linked with other clusters.

Cluster: Gh0st



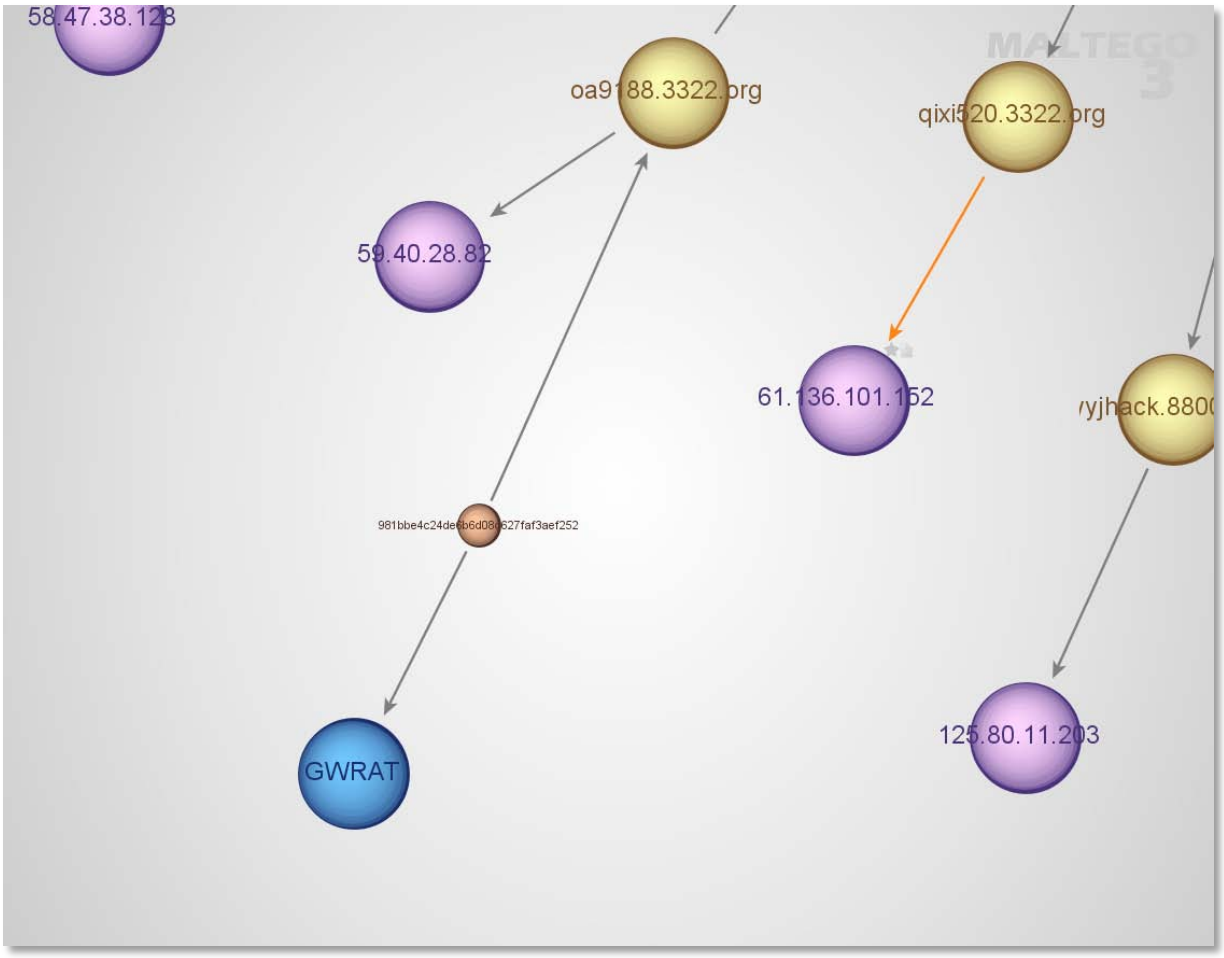
The Gh0st cluster is by far the largest with 522 samples in the test set. Since this is the default configuration, not much relational information can be inferred from it, even if it shares links with many of the other clusters.

Cluster: GOLDt

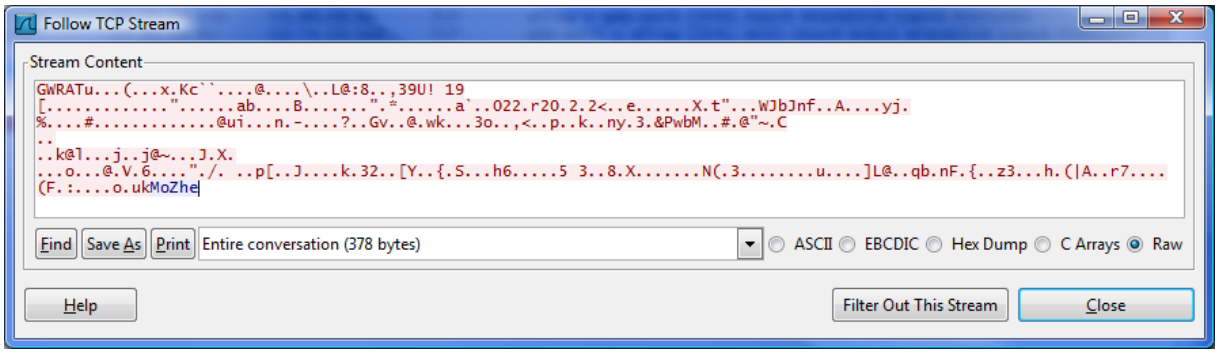


The GOLDt cluster contains one sample, and appears not linked with other clusters.

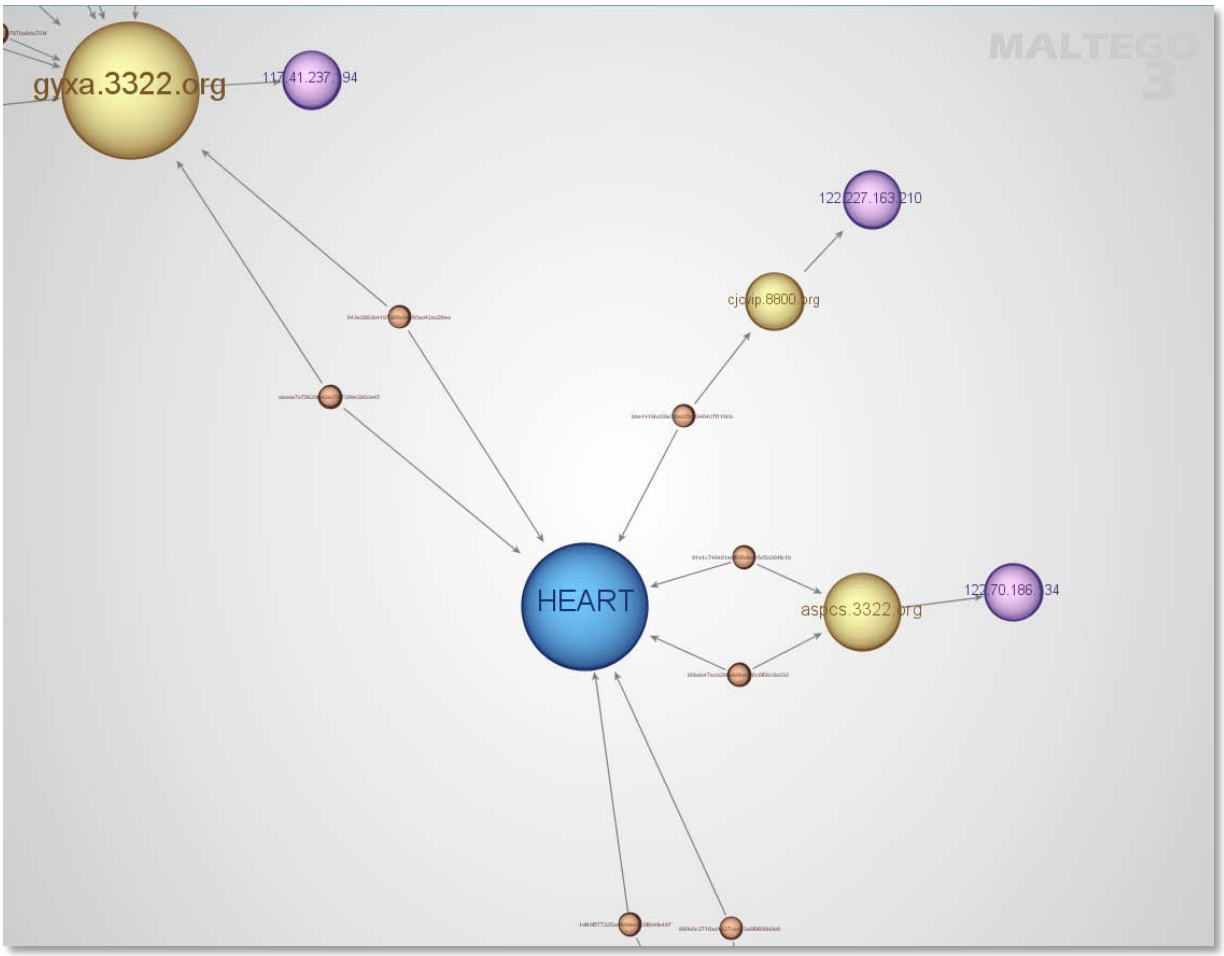
Cluster: GWRAT



The GWRAT cluster contains one sample, and is linked to the MoZhe cluster through returned traffic from its C&C server oa9188.3322.org.

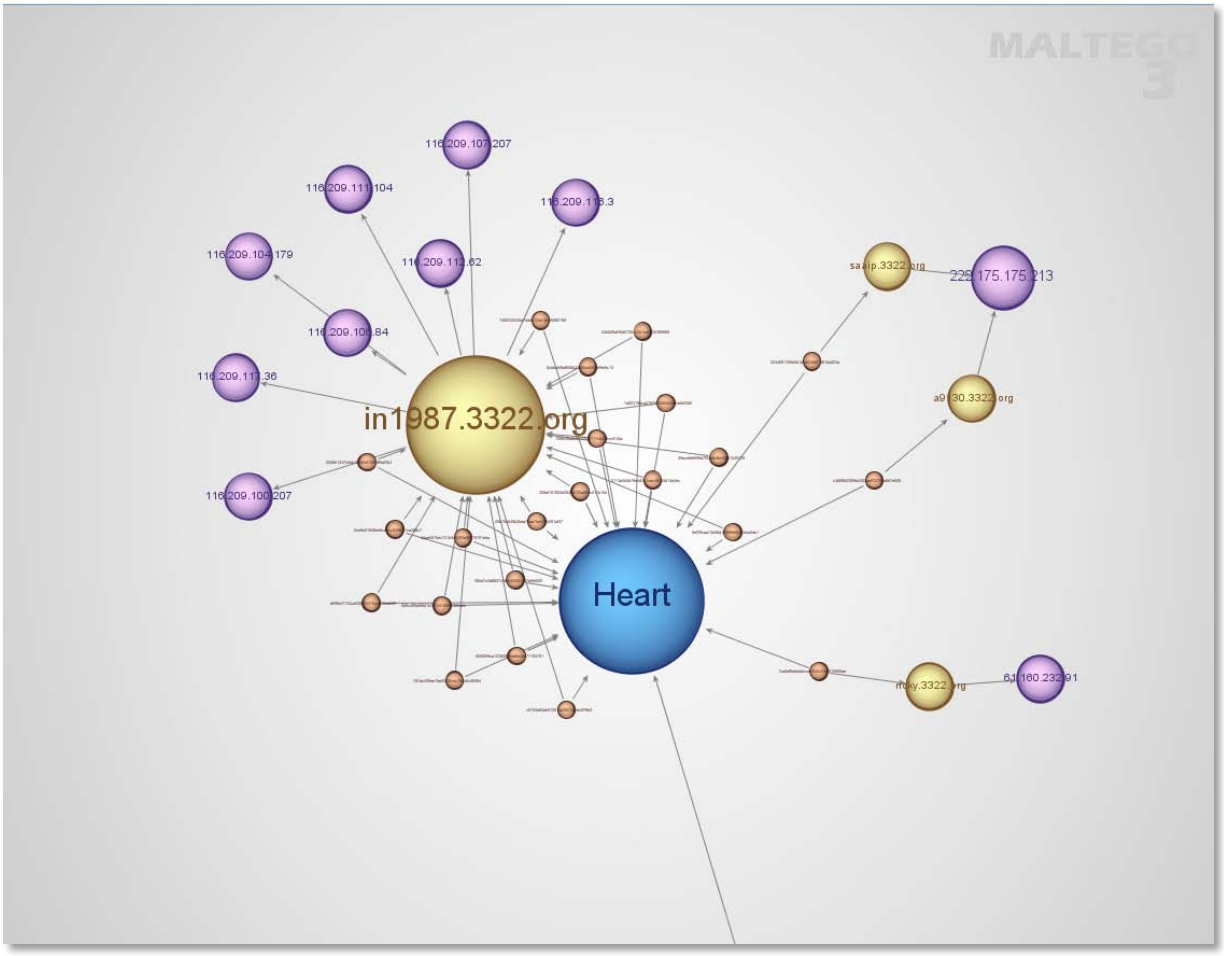


Cluster: HEART



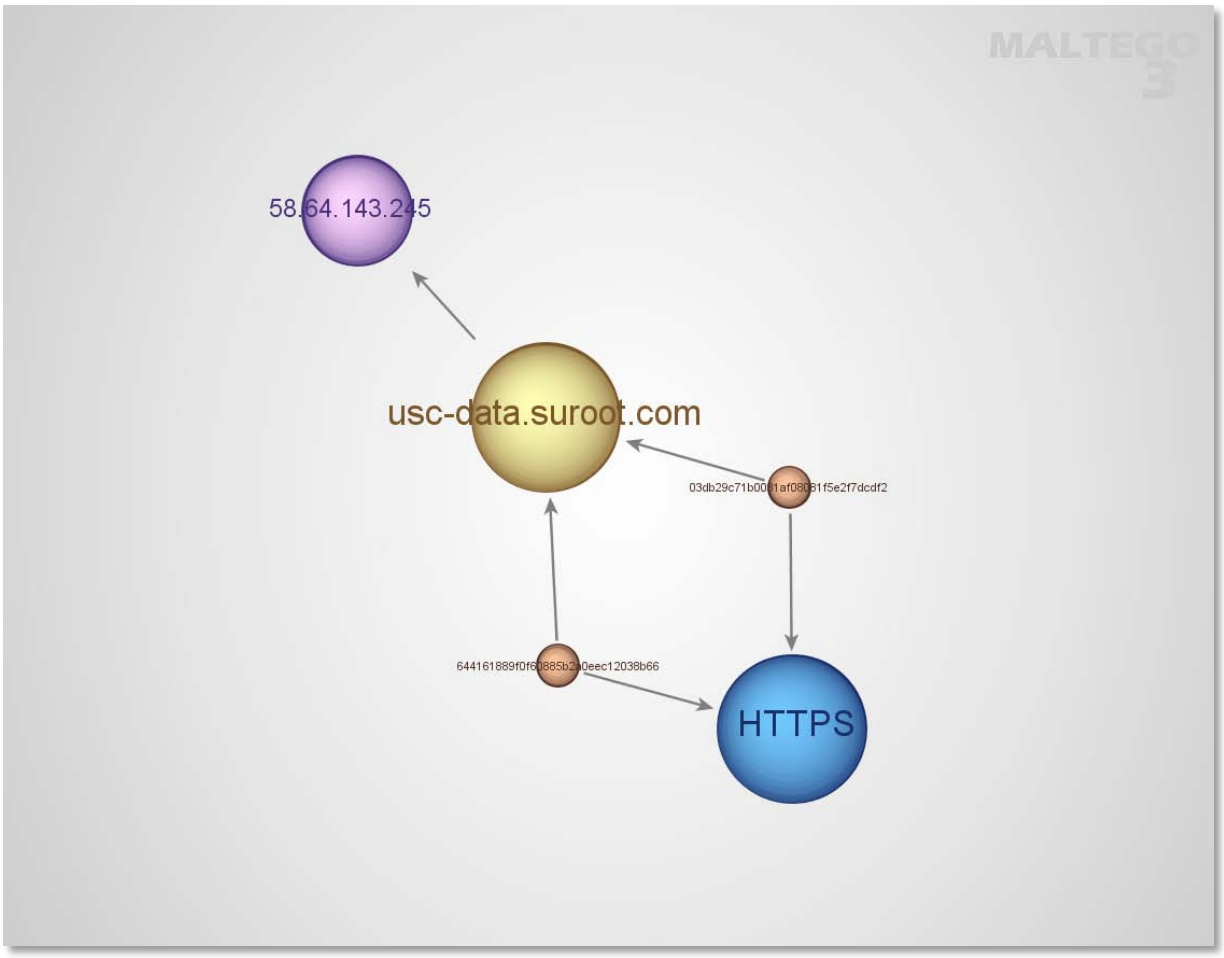
There are 7 samples in the HEART cluster. HEART links with KOBBX through common C&C at gyxa.3322.org. It also links with the PCRat cluster through a common IP at 60.190.219.234.

Cluster: Heart

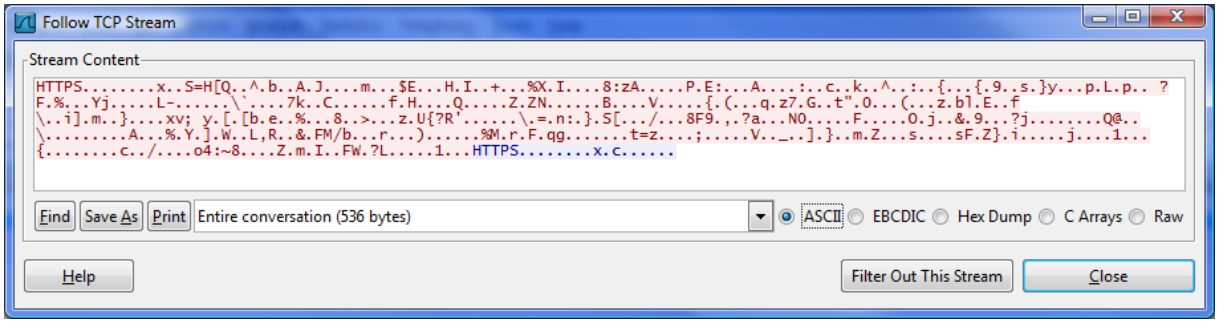


The Heart cluster consists of 26 samples, and is connected with the main Gh0st cluster through the C&C at wangyanlei.3322.org. Some of these samples (the ones connecting to in1987.3322.org and saaip.3322.org) use uncompressed communication, which is unusual for Gh0st Rat.

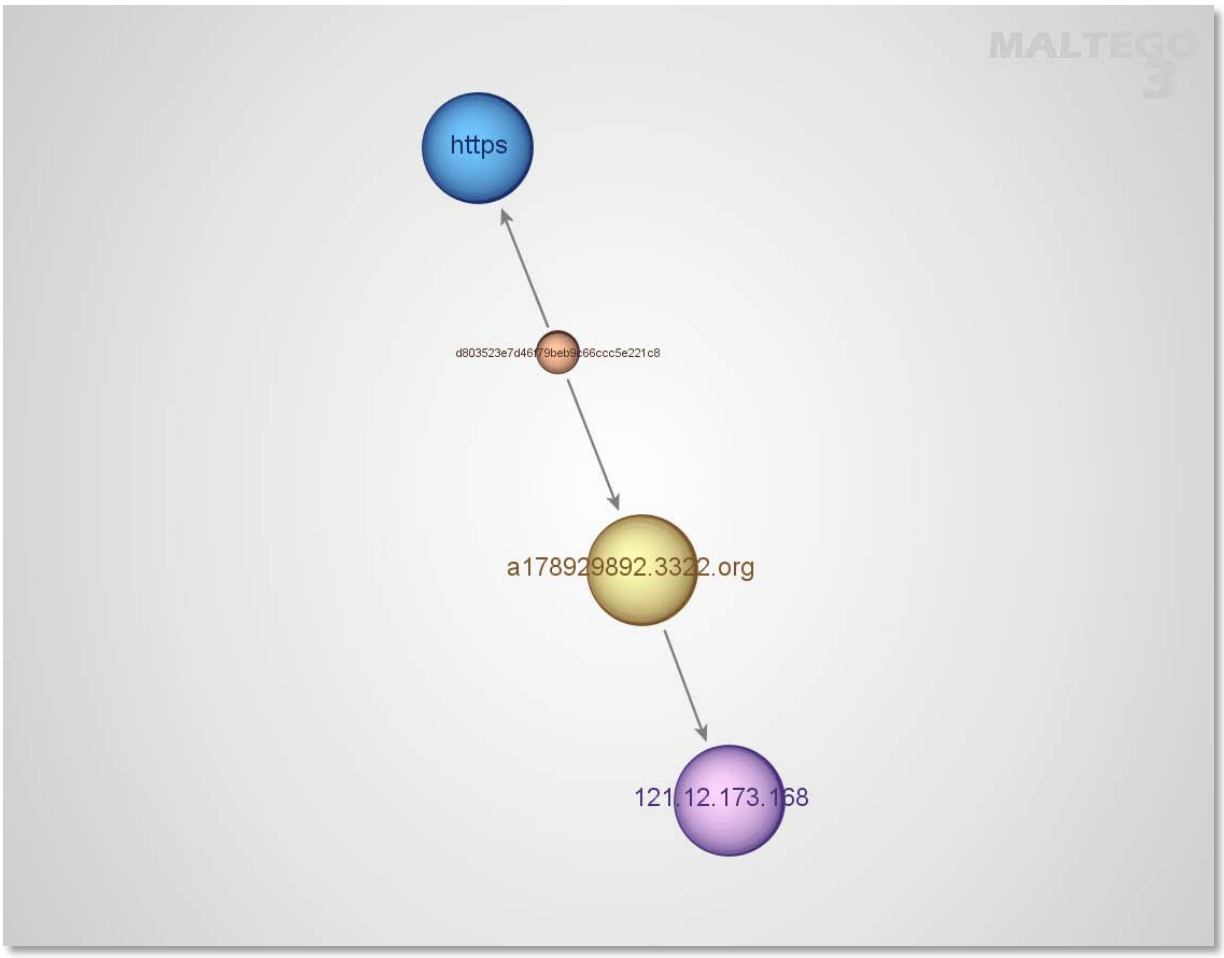
Cluster: HTTPS



There are two samples in this cluster, but we see no further links with other clusters.

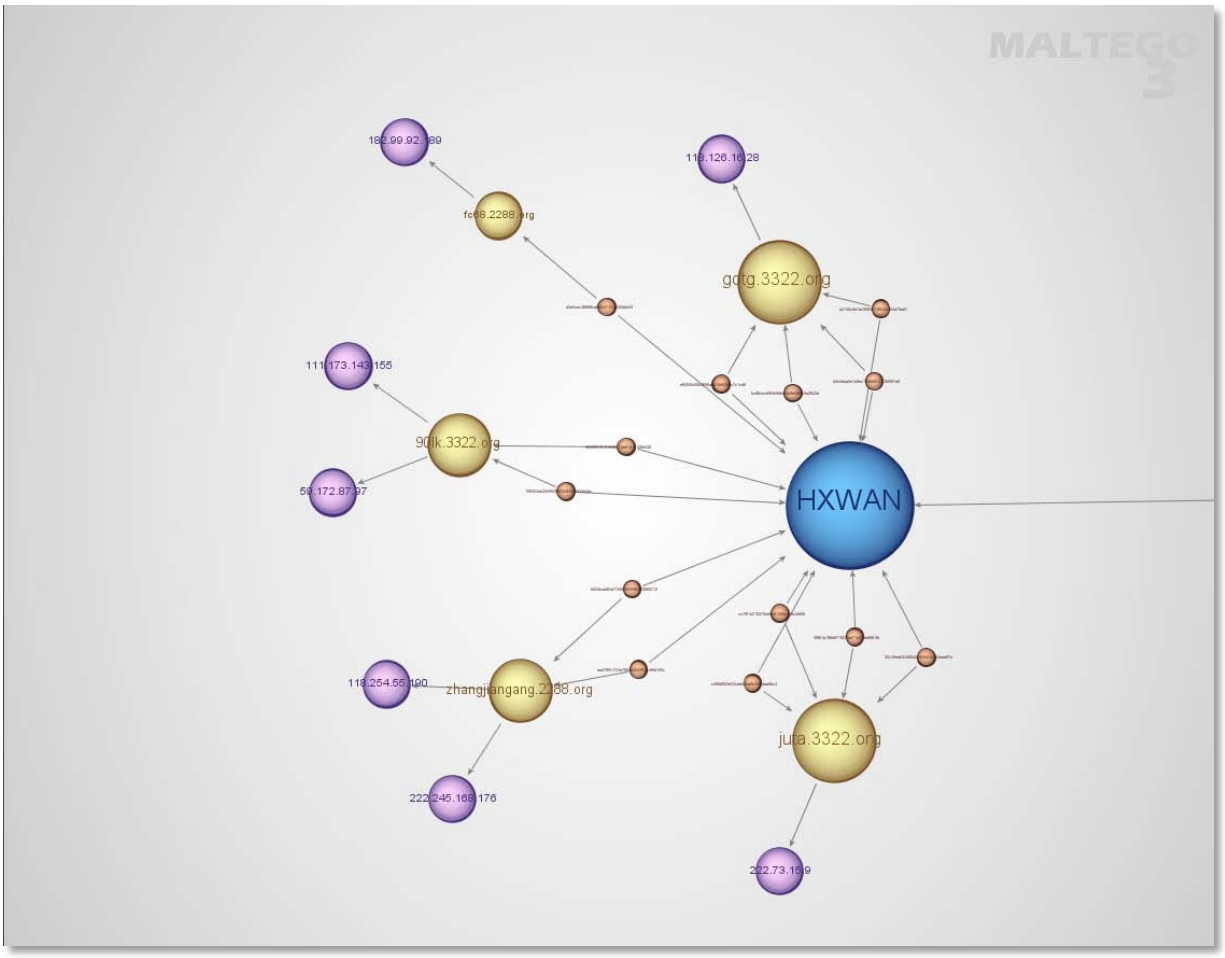


Cluster: https



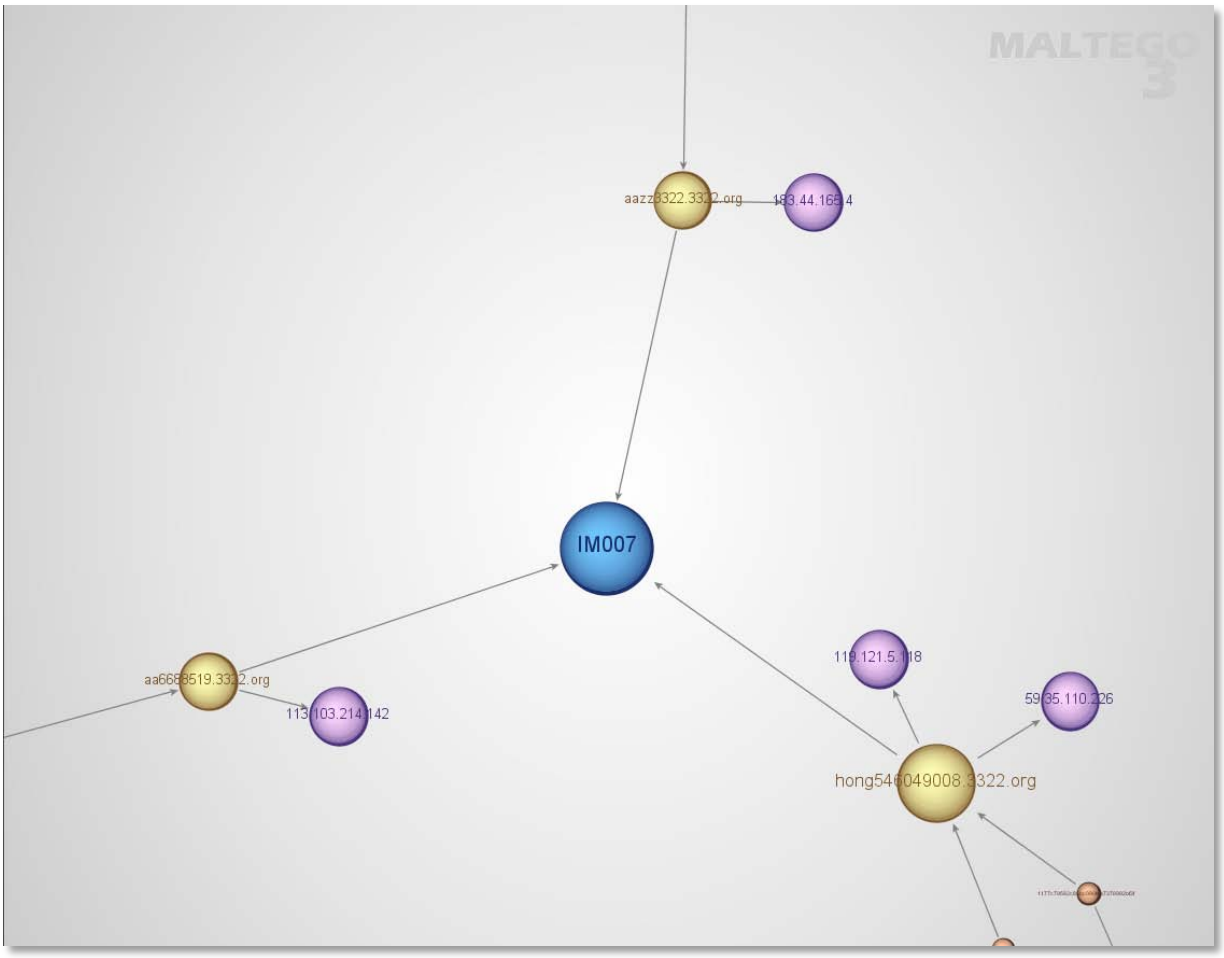
The https cluster contains one sample, and appears not linked with other clusters.

Cluster: HXWAN



The HXWAN cluster consists of 14 samples. It is linked with the KrisR, Lyyyy and XDAPR clusters (See KrisR).

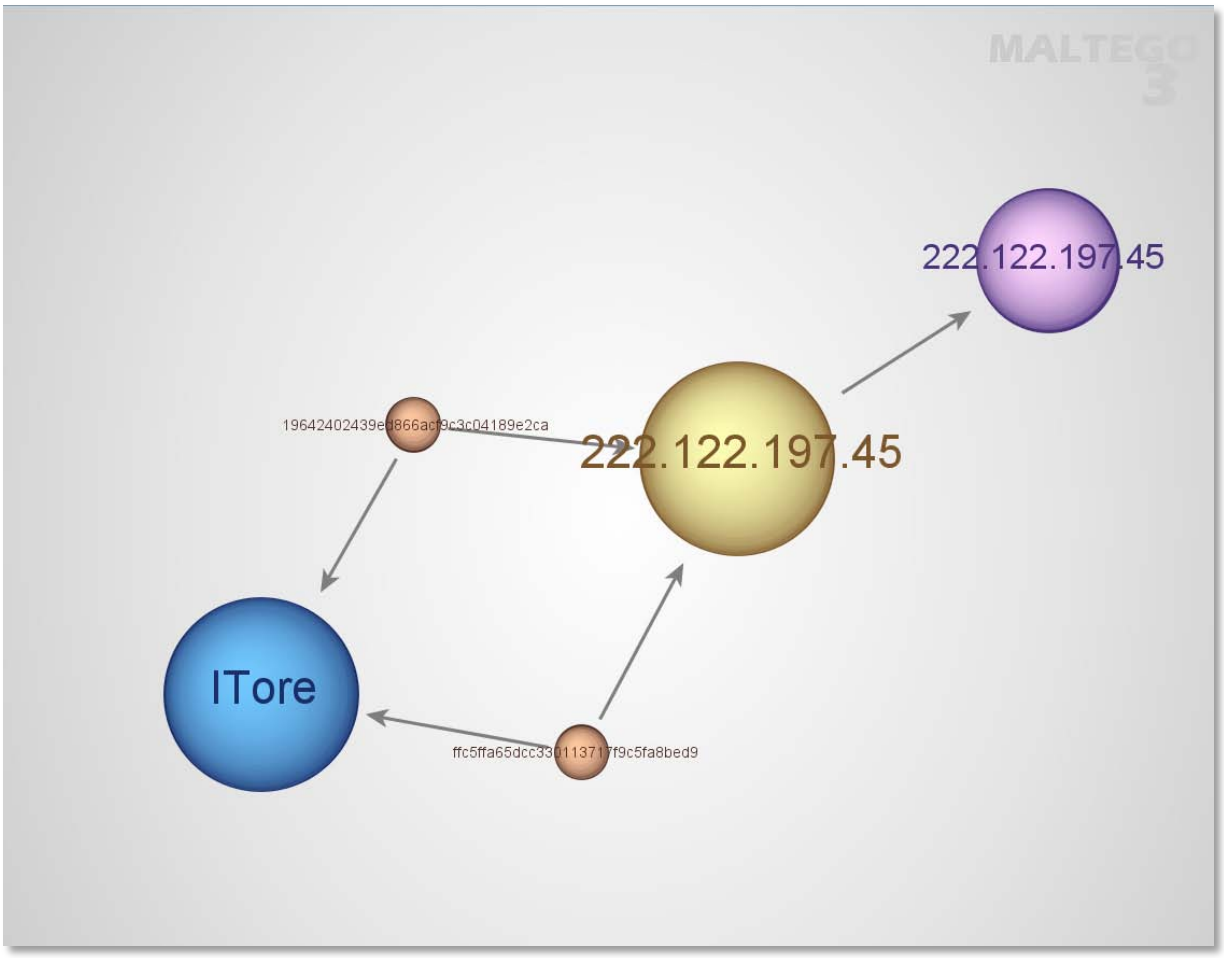
Cluster: IM007



The IM007 cluster surprisingly contains **no** samples. The reason it exists at all is that we have logged several C&C servers *replying* with this magic tag, so it is a reasonable assumption that there must exist samples that follow this protocol. The servers we have seen with this behavior have been used by the BeiJi, BEiLa and Wangz clusters, thus linking these.
In at least two cases we have seen samples from these clusters showing images of *Dungeon Fighter Online* virtual items when run, apparently as a lure for game account theft.

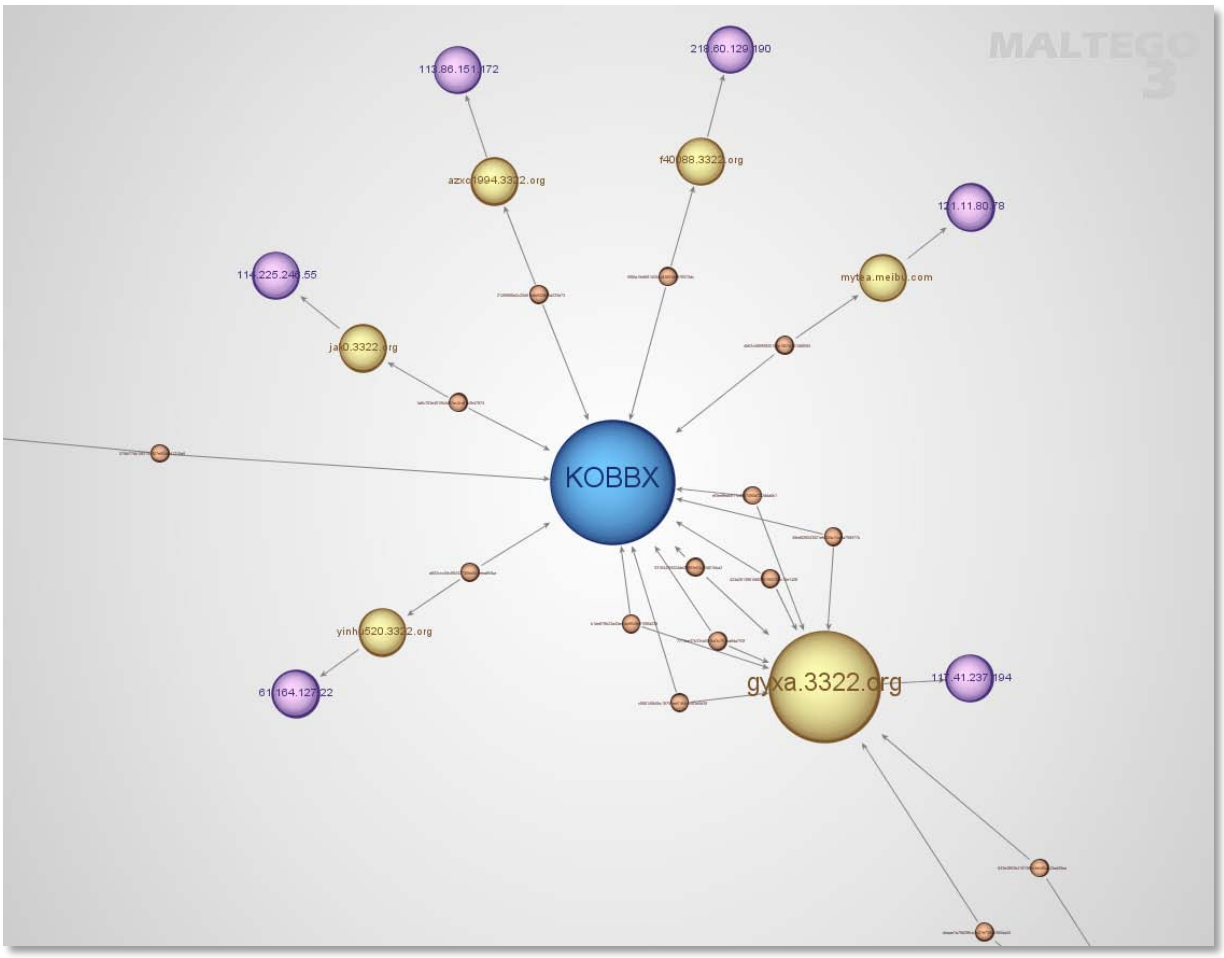
Bamboo Bracelet, an expensive ingame item in DFO.

Cluster: ITore

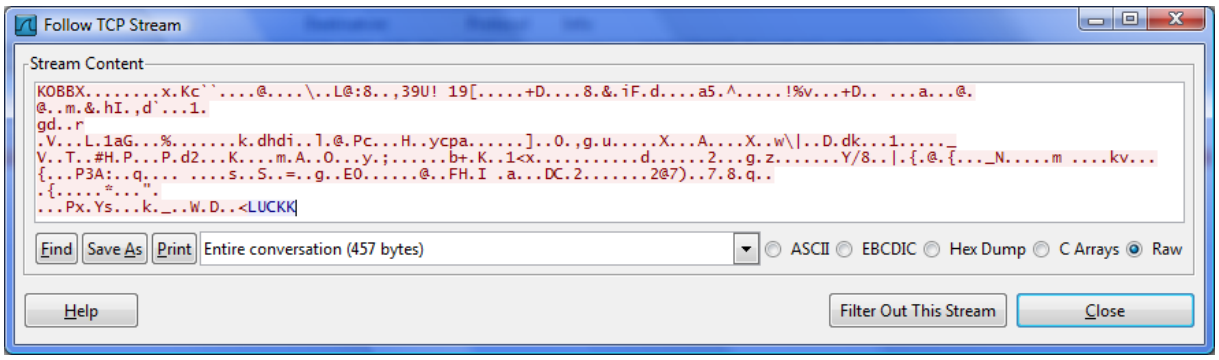


The ITore cluster appears unconnected to other clusters. The executables are significantly different from other Gh0st Rats and may be another family altogether, even if the communication is similar.

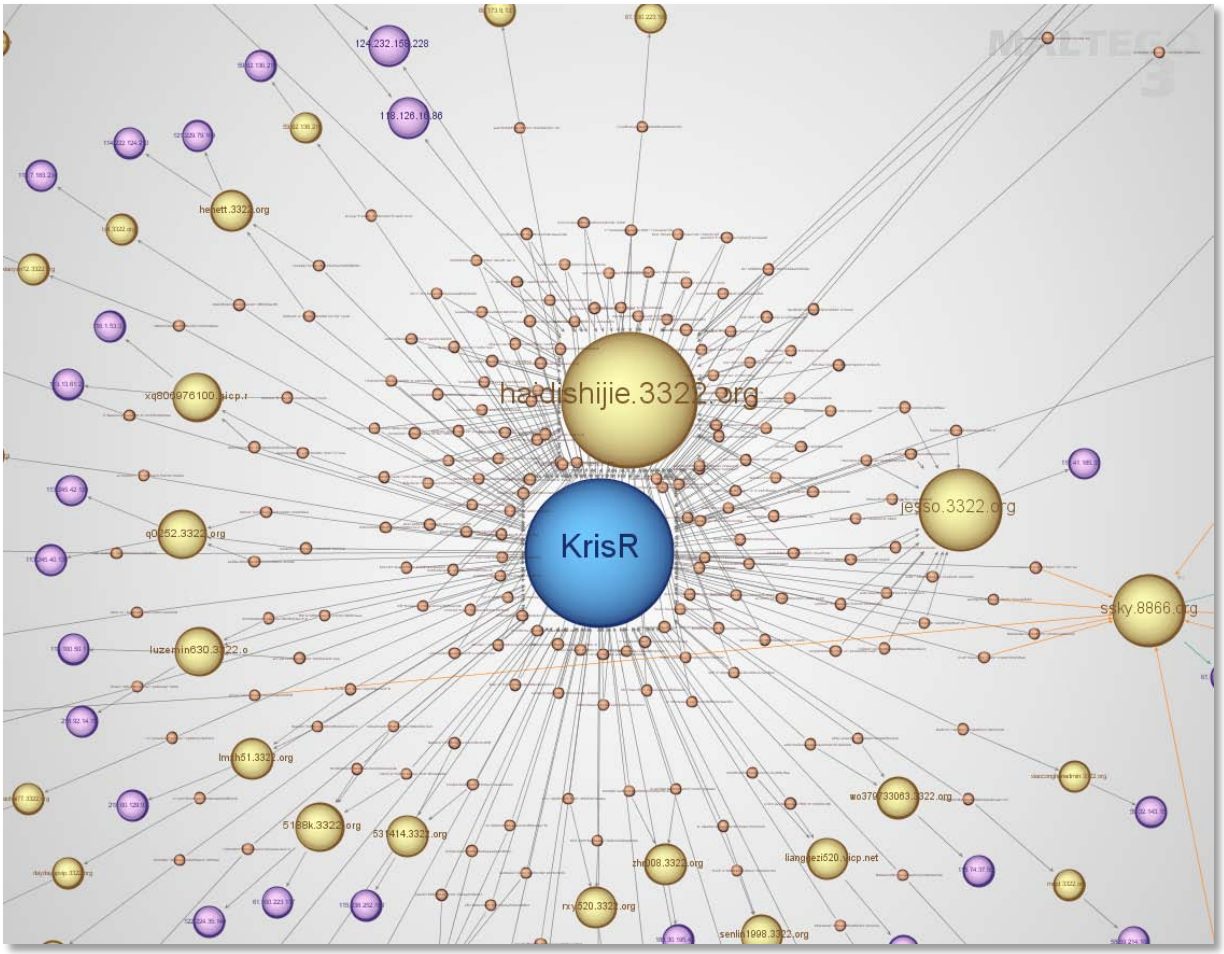
Cluster: KOBBX



The KOBBX cluster consists of 13 samples in the set. It is linked with the HEART cluster through the common C&C at gyxa.3322.org, and to the LUCKK cluster through miscommunication from wjdl.3322.org.



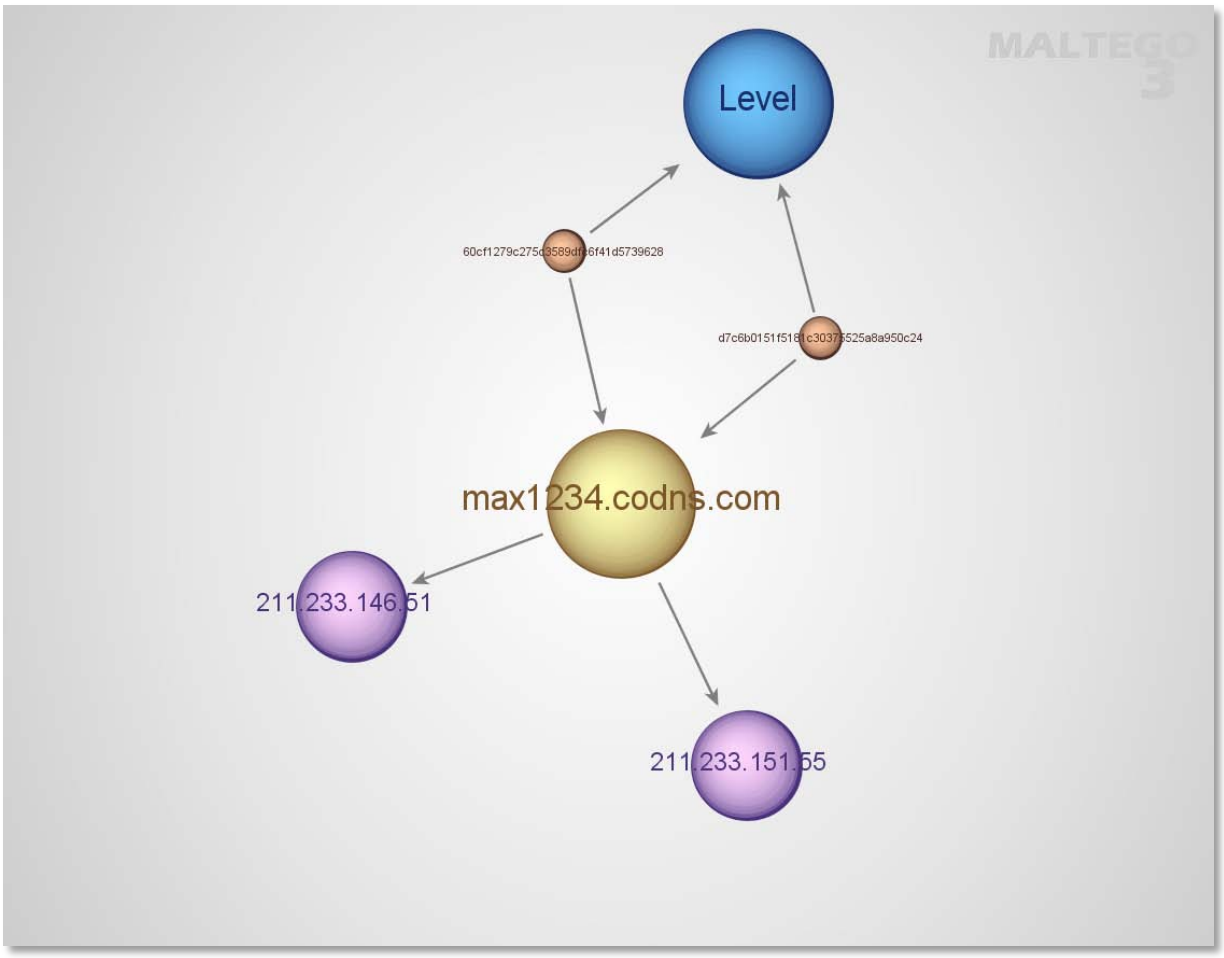
Cluster: KrisR



The KrisR cluster consists of 205 samples. The magic tag is actually “KrisRat”, but the tag is truncated in traffic to the regular first 5 bytes.

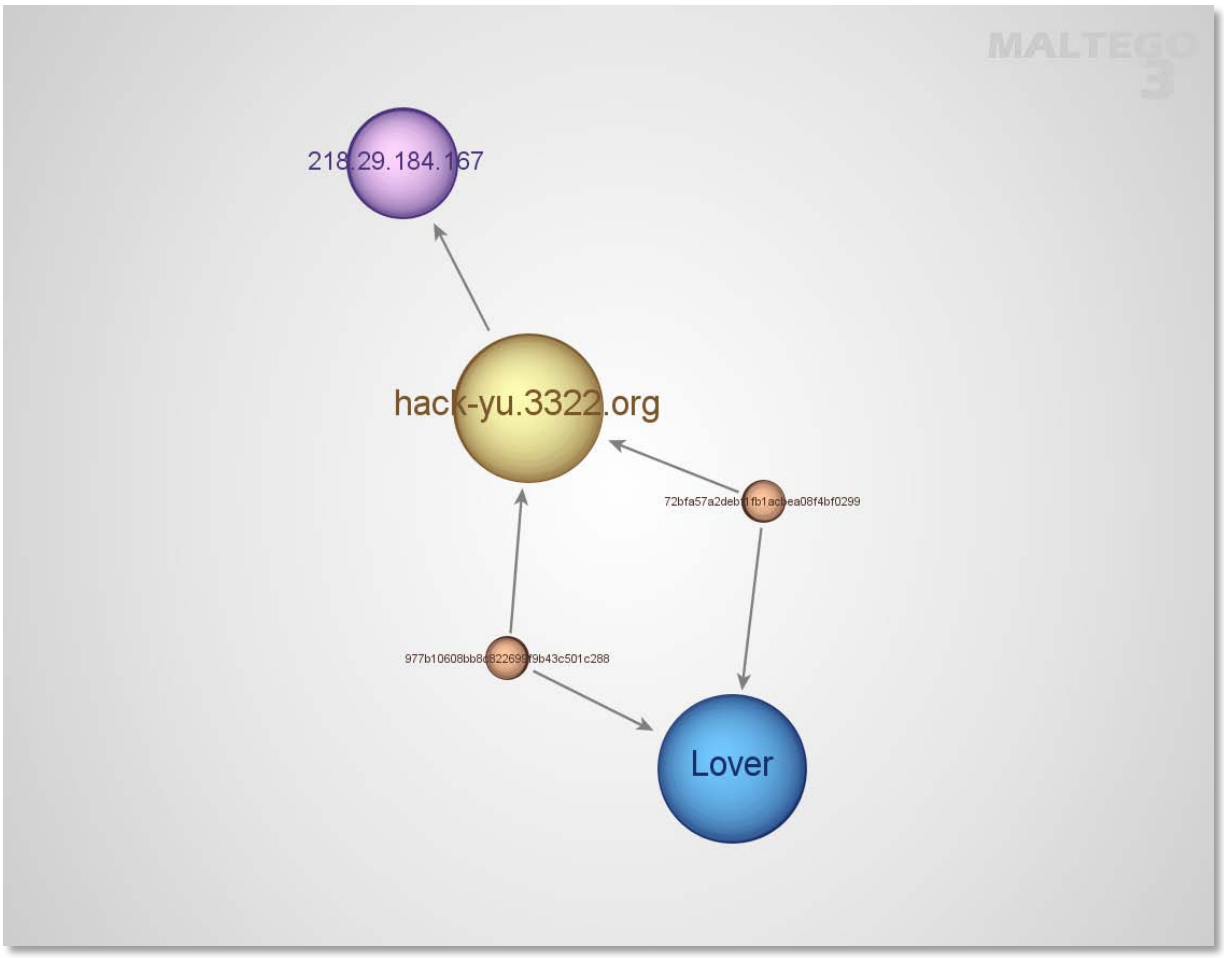
By far most samples connect back to haidishijie.3322.org, but many other C&C’s are in use. This cluster links with:
FLYNN: see FLYNN
Gh0st: f. ex. haidishijie.3322.org returned ‘Gh0st’ in all cases when receiving ‘KrisR’ on port 8888
HXWAN: common C&C at ssky.8866.org
Lyyyy: common C&C at ssky.8866.org
XDAPR: common C&C at ssky.8866.org
cb1st: common C&C at daduji.3322.org
FKJP3: common C&C at daduji.3322.org

Cluster: Level



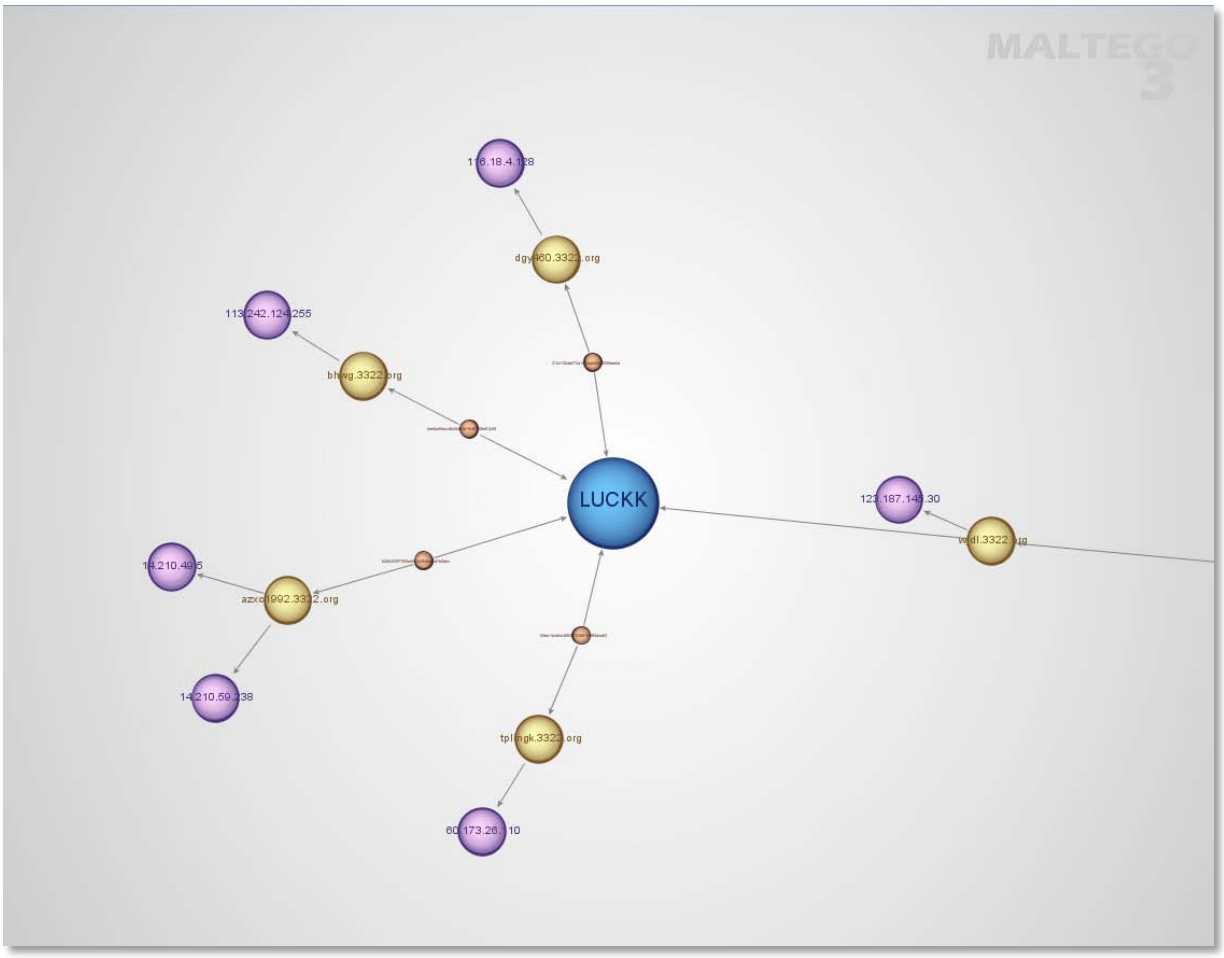
The Level cluster consists of two samples. It appears unlinked with other clusters.

Cluster: Lover



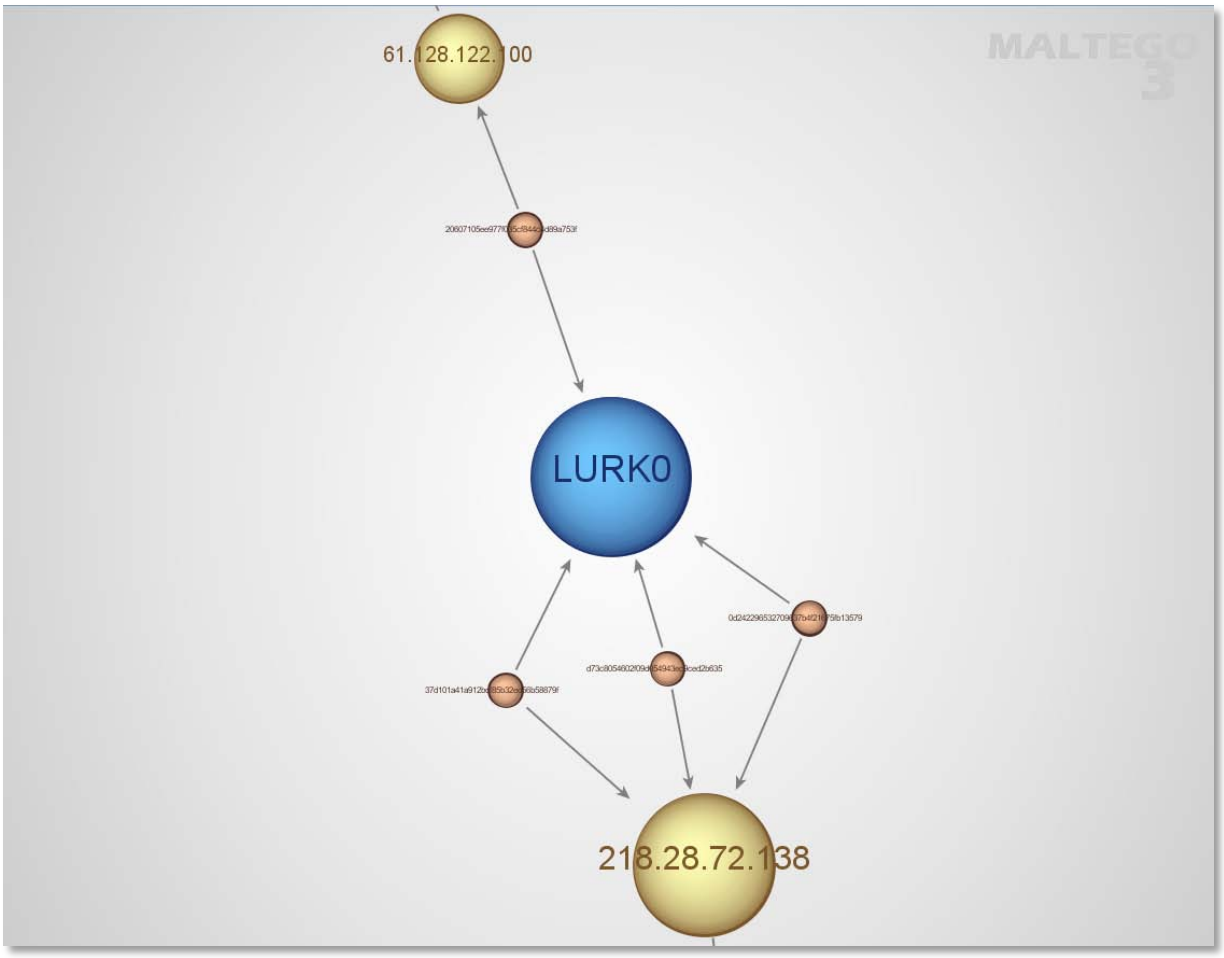
The Lover cluster consists of two samples. It appears unlinked with other clusters.

Cluster: LUCKK



The LUCKK cluster consists of four samples in the set. It is linked with the KOBBX cluster though communication (see KOBBX).

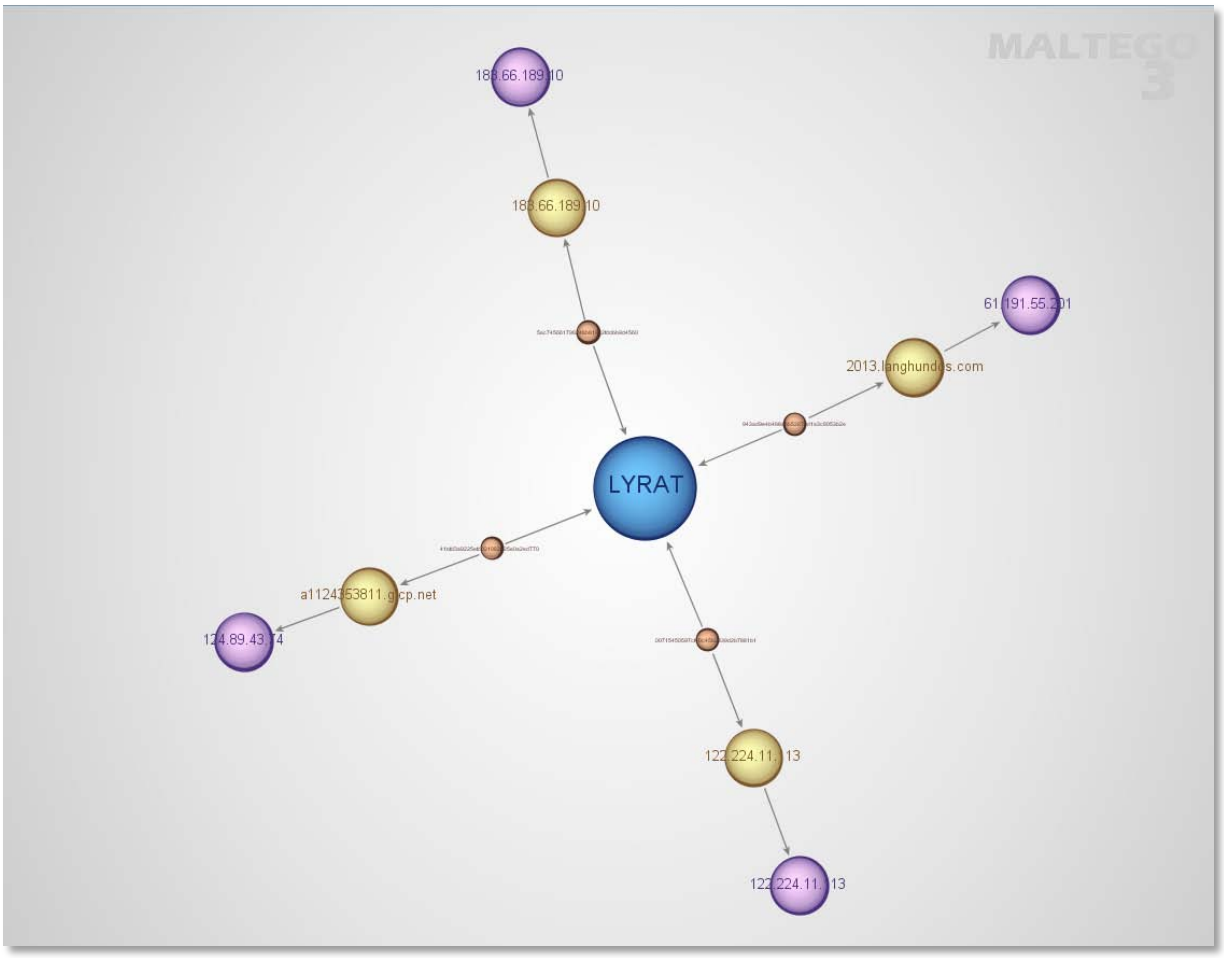
Cluster: LURK0



The LURK0 cluster consists of four samples in the set. This cluster was documented as connected with the SK Communications breach in South Korea in 2011 (8), and has been seen used against Tibetan groups (9), (10).

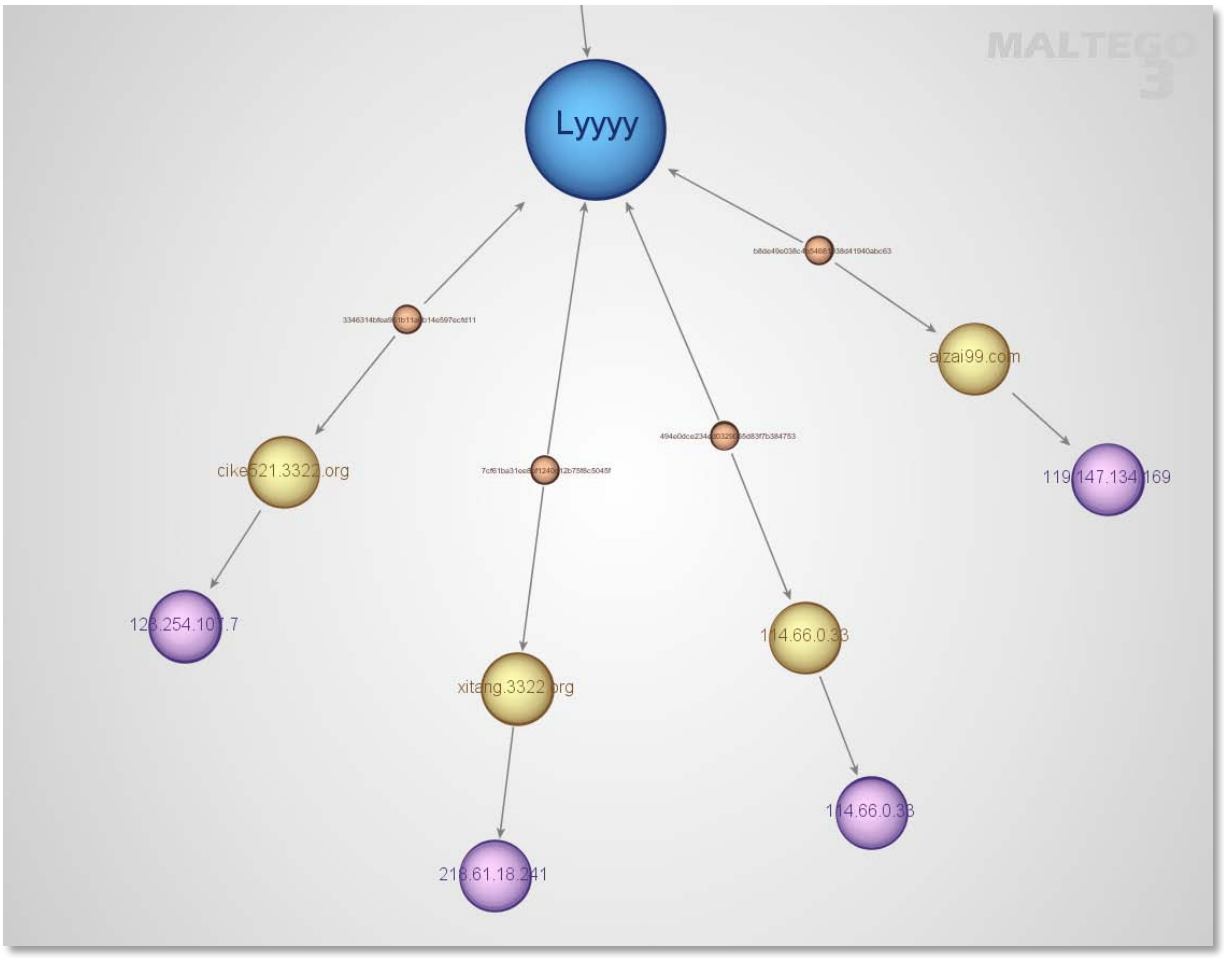
It is also linked with the OXXMM cluster through the usage of a common C&C at the hardcoded IP 218.28.72.138.

Cluster: LYRAT



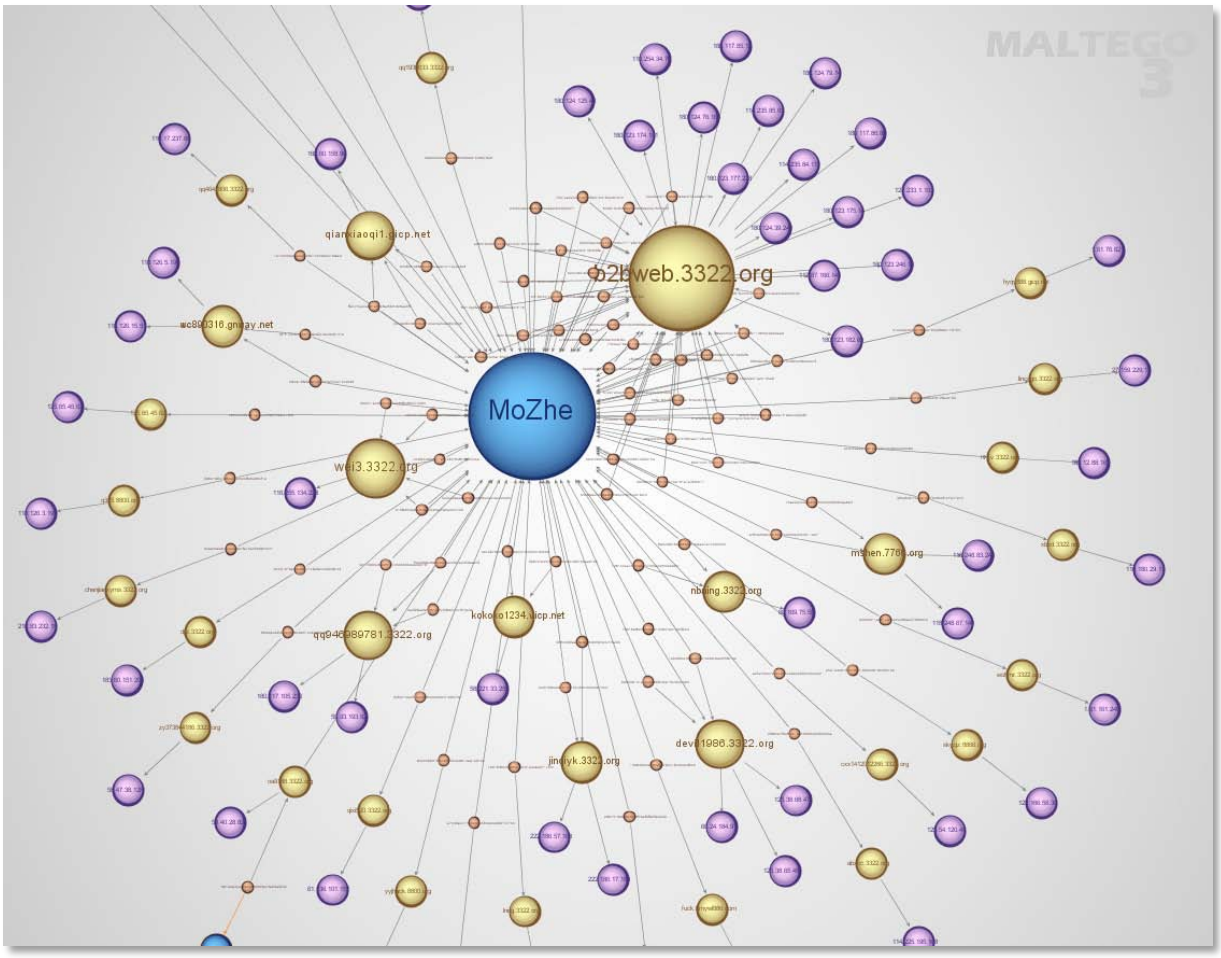
The LYRAT cluster consists of four samples. It appears unconnected with other clusters.

Cluster: Lyyyy



The Lyyyy cluster consists of 4 samples. It is linked with the KrisR, HXWAN and XDAPR clusters (See KrisR).

Cluster: MoZhe



This cluster consists of 87 samples. Most of these connect back to b2bweb.3322.org. MoZhe is linked with

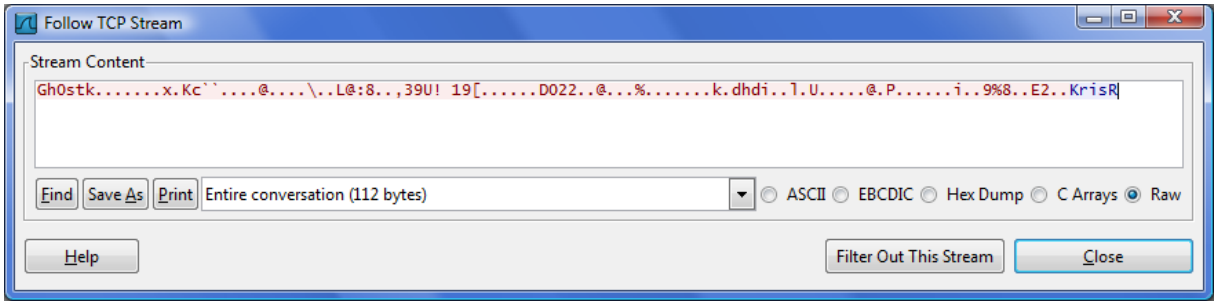
X6RAT: common C&C at ingalar.3322.org

Winds: common C&C at hkl8973875.3322.org

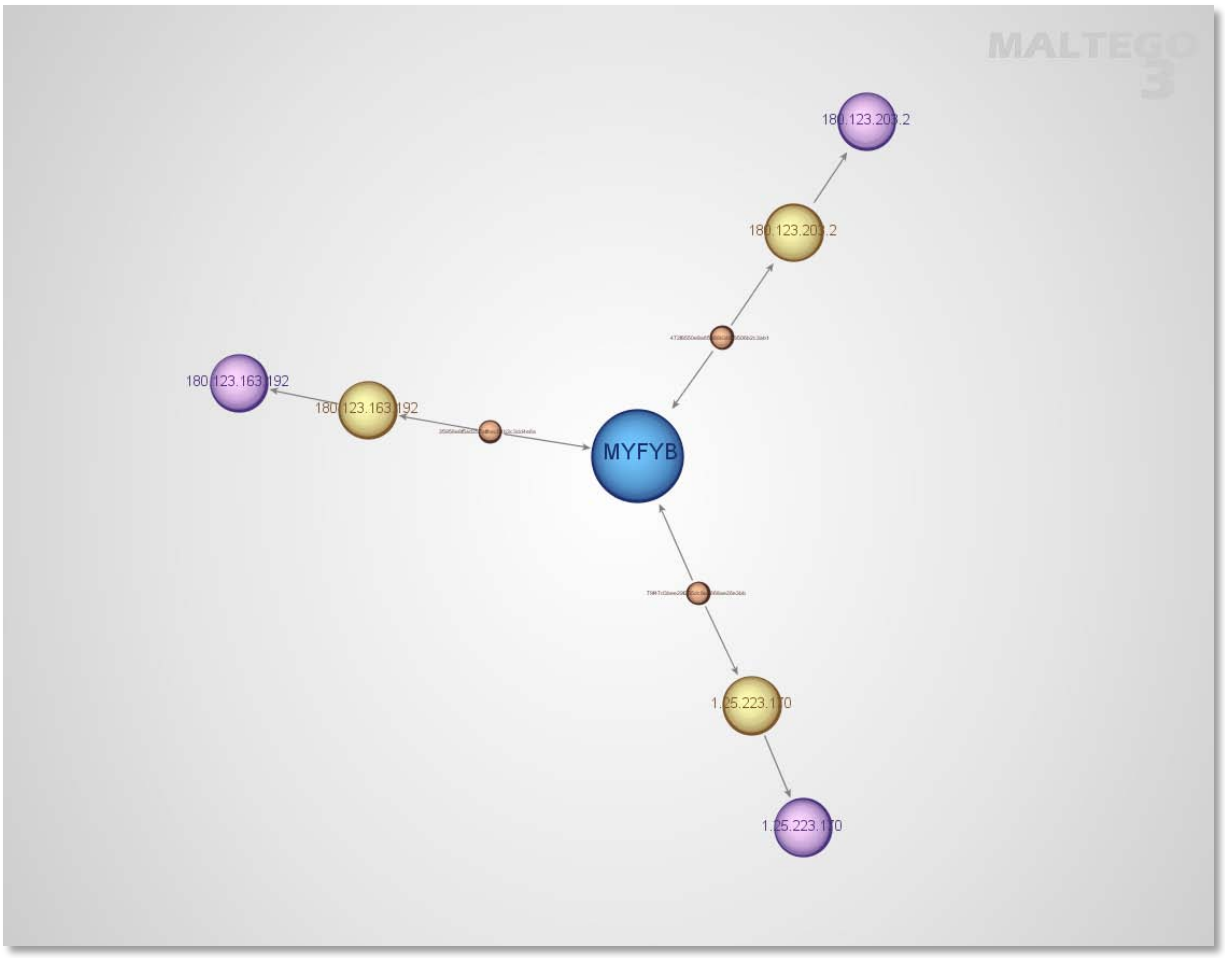
Additional links are seen through observed traffic.

GWRAT: The GWRAT C&C oa9188.3322.org replies with MoZhe (See GWRAT)

KrisR: The MoZhe C&C at ingalar.3322.org replies with KrisR:

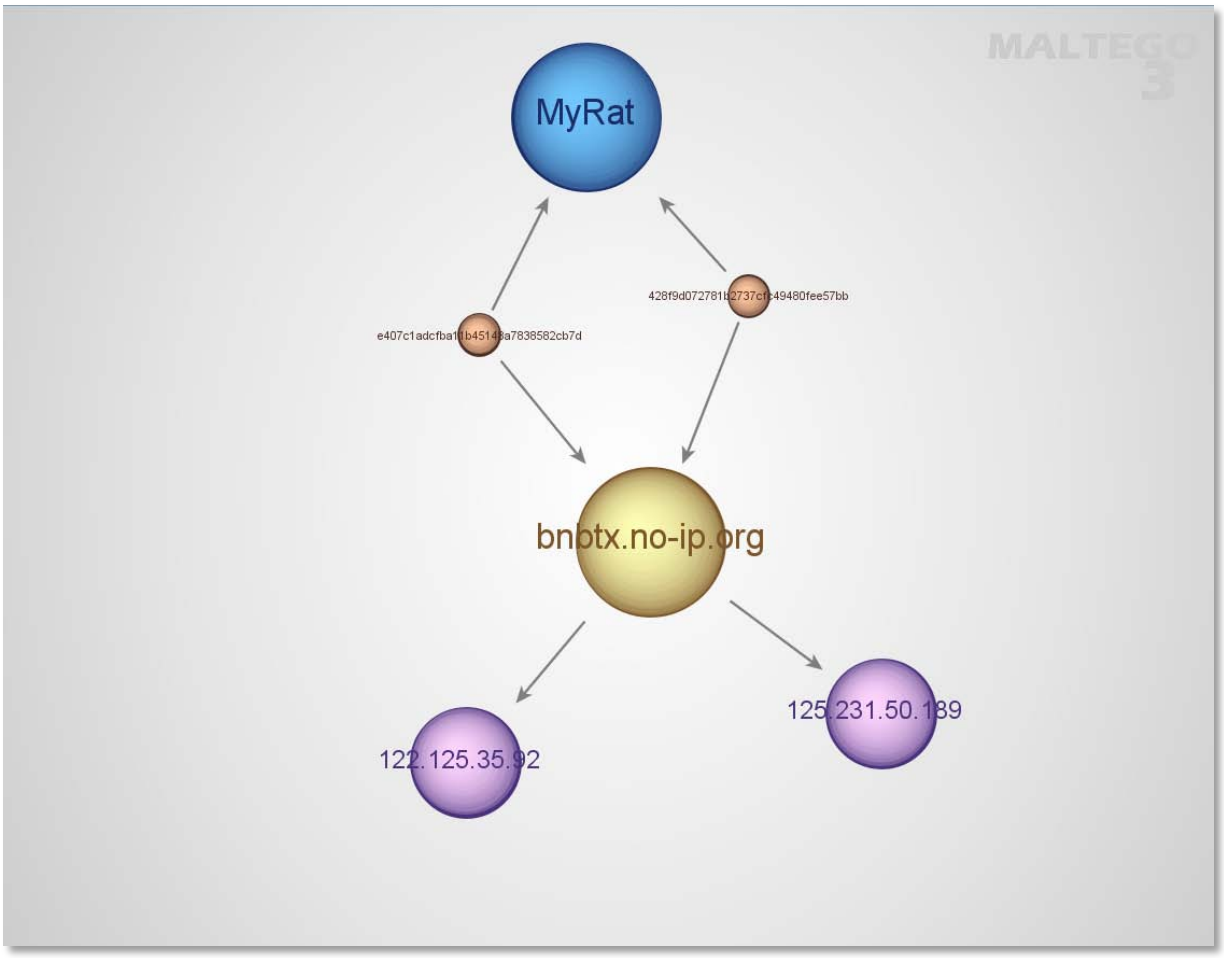


Cluster: MYFYB



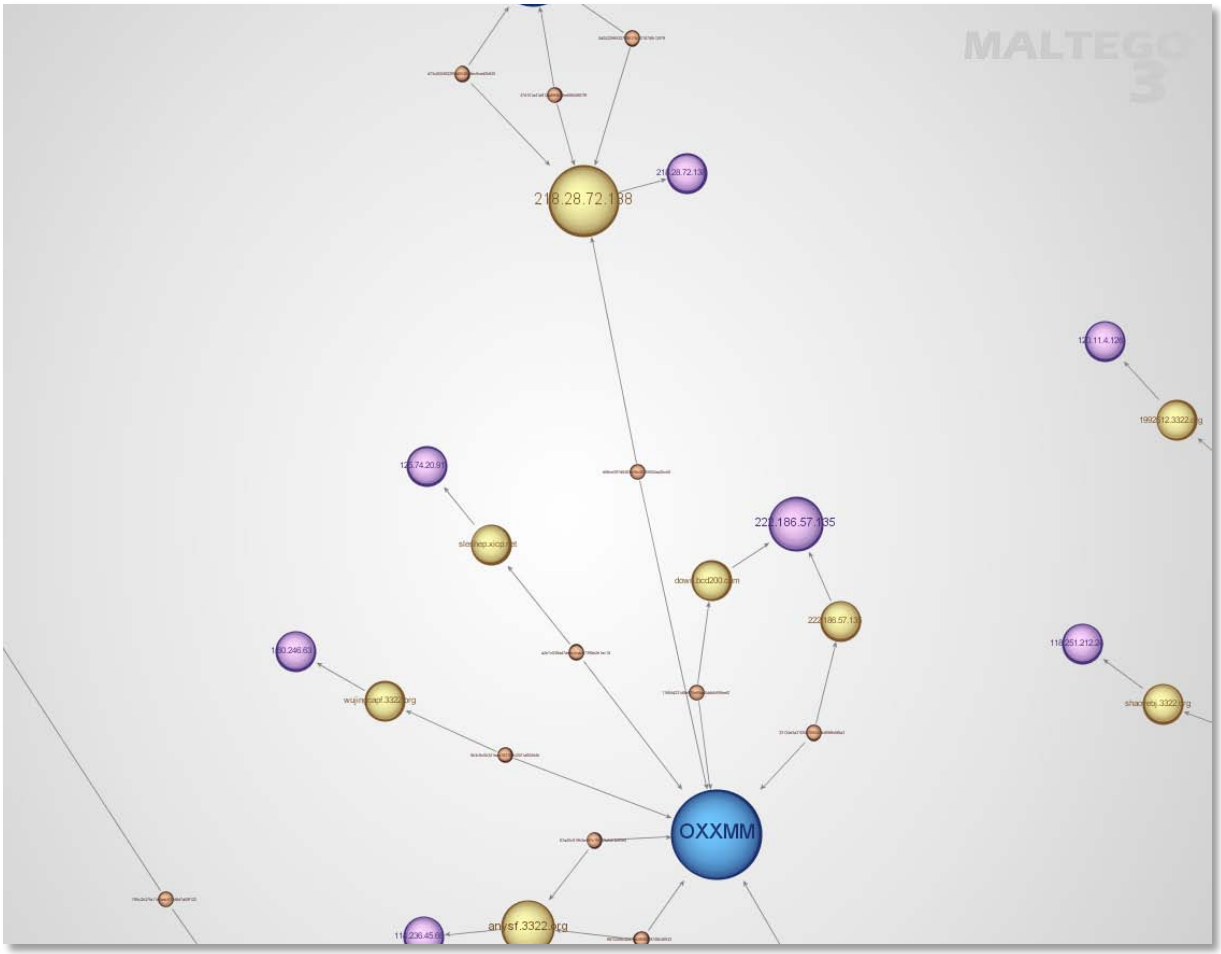
The MYFYB cluster contains three samples. It does not appear connected with other clusters.

Cluster: MyRat



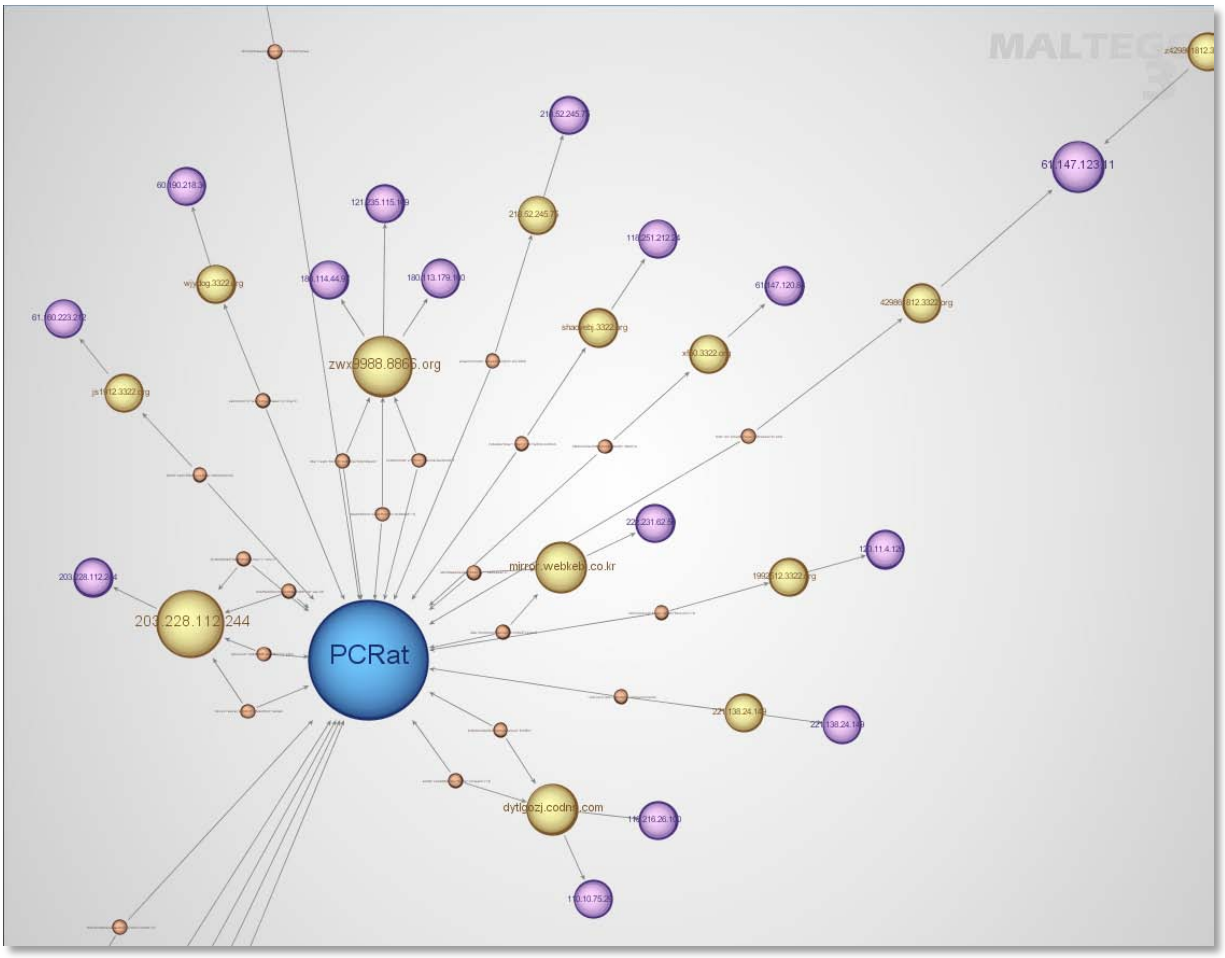
The MyRat cluster contains two samples. It appears unconnected with other clusters.

Cluster: OXXMM



The OXXMM cluster contains eight samples. It connects with the Gh0st main cluster through common C&C at a6422563.vicp.net and to the LURK0 cluster through common C&C at 218.28.72.138.

Cluster: PCRat

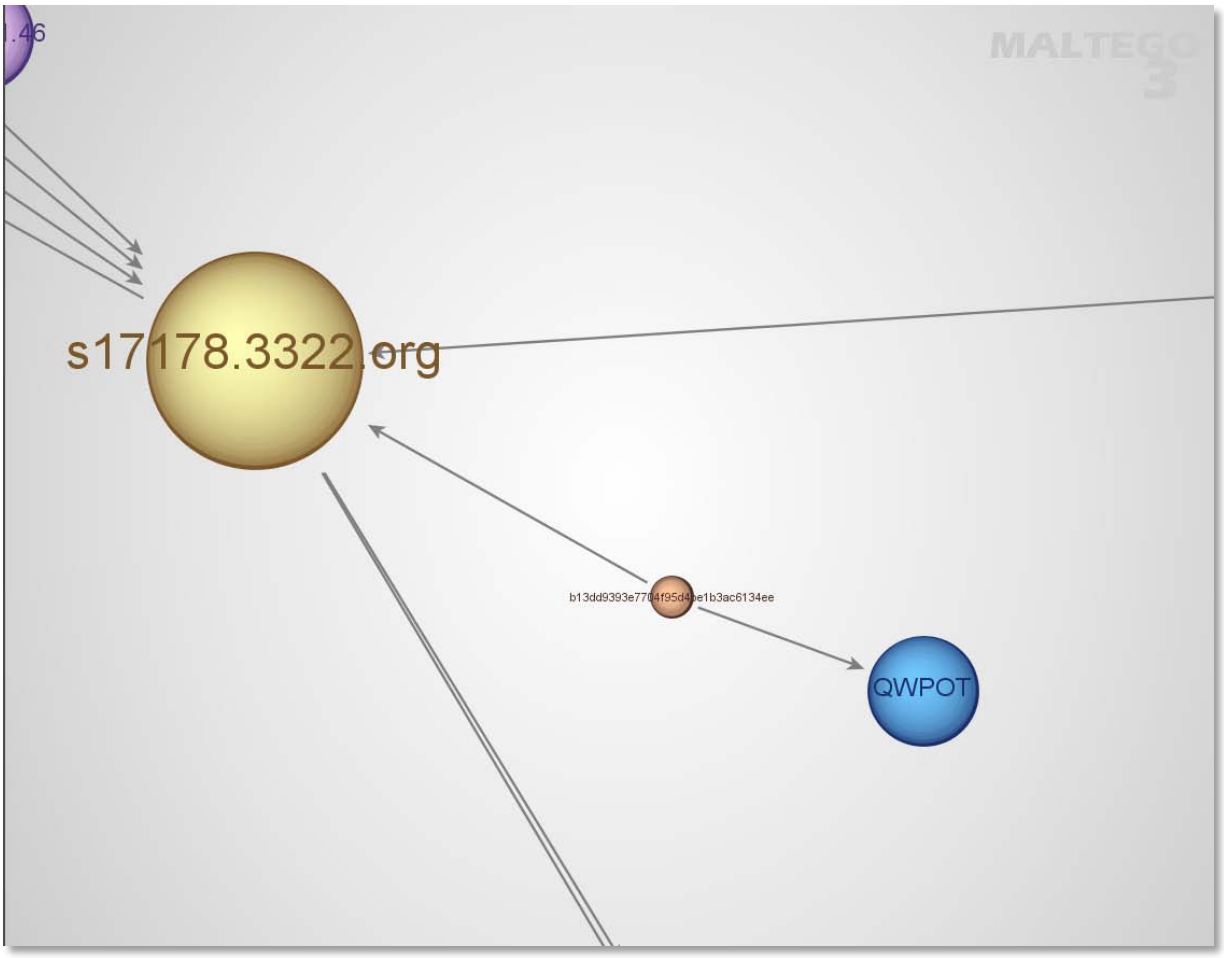


This cluster contains 25 samples, and is linked with the HEART cluster (see HEART), the 7hero cluster (see 7hero) as well as the main Gh0st cluster through the common C&C at tajs.3322.org. It is also linked to the Winds cluster through common C&C at mstsc5.3322.org.

PCRat samples have been documented used against Uyghur groups (11).

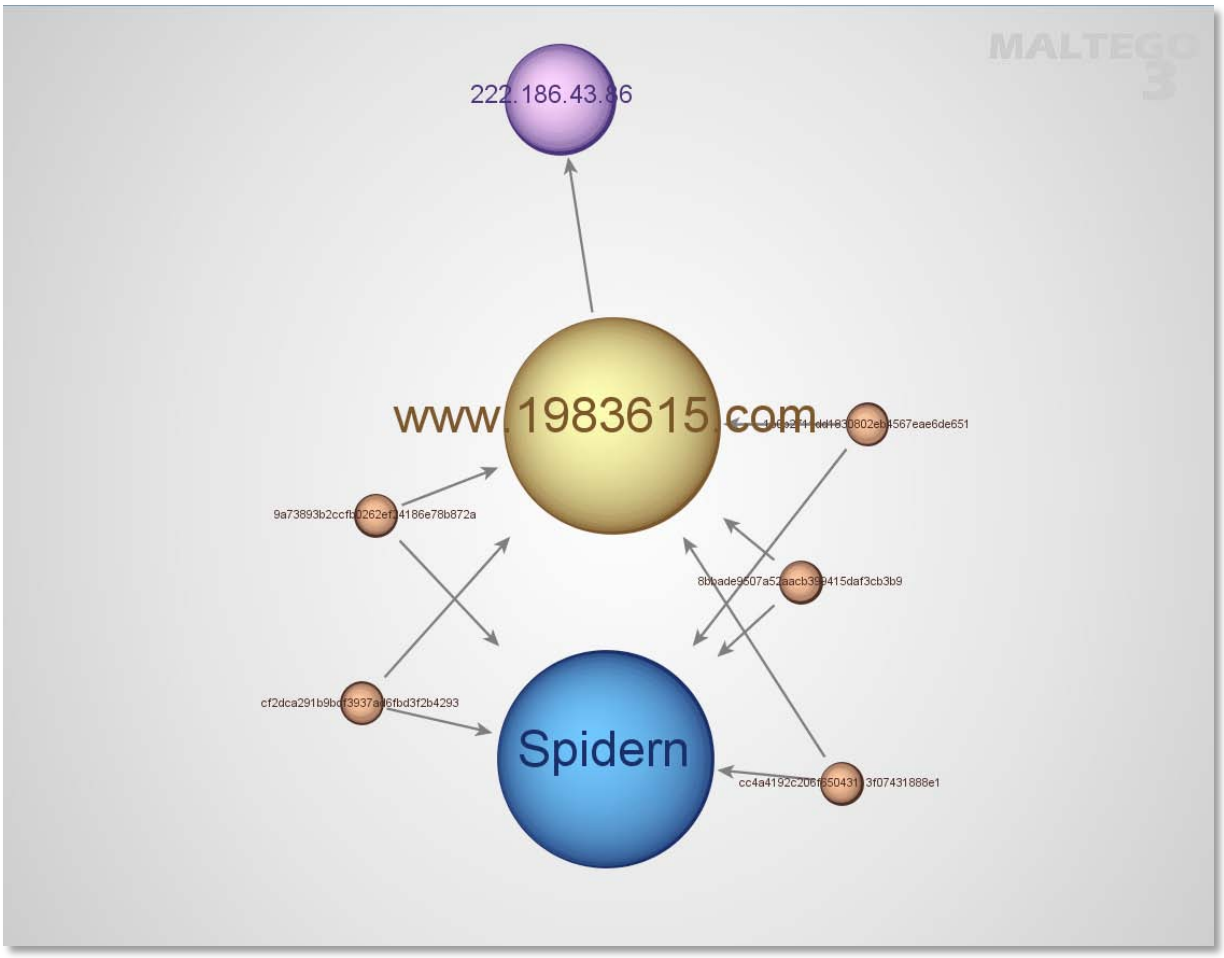
It is debatable how valid the PCRat connections are. There is apparently a commercially available modification of Gh0st rat called PCRat, which we have not yet seen copies of. If that kit uses the PCRat magic tag as there is reason to suspect, this cluster is of little value.

Cluster: QWPOT



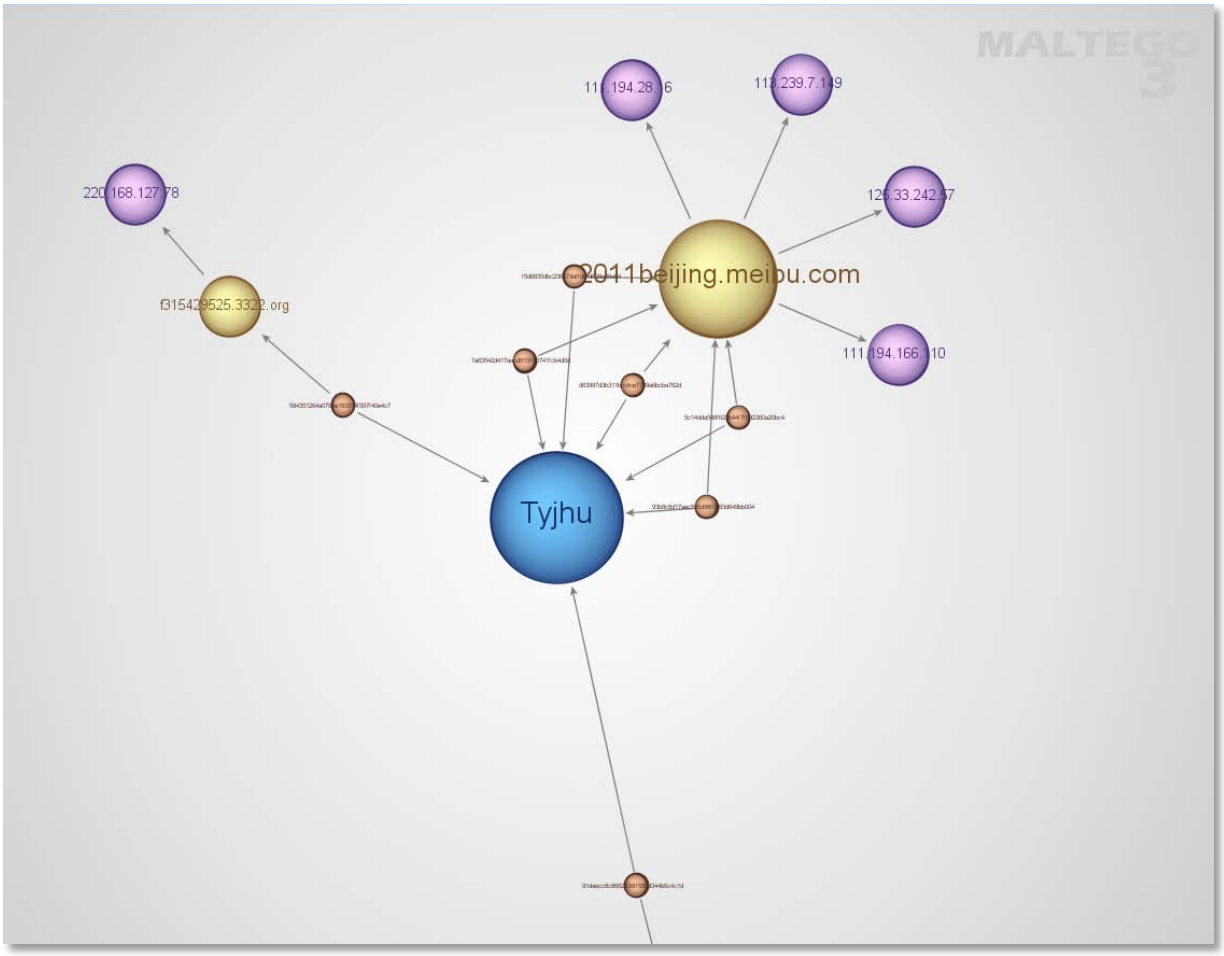
The QWPOT cluster contains only one sample. It is connected to the Xjjhj and Gh0st clusters through its C&C at s17178.3322.org.

Cluster: Spidern



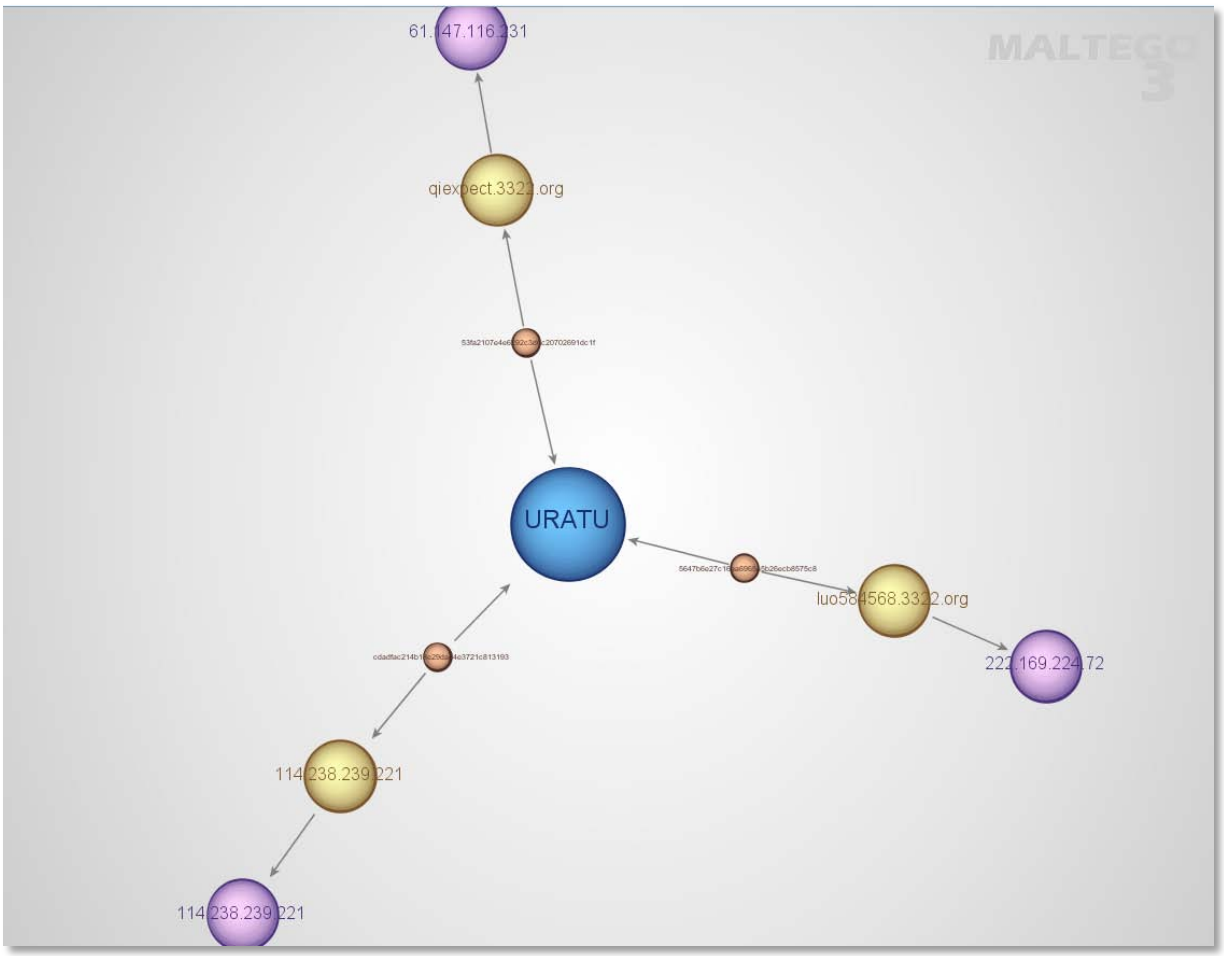
The Spidern cluster consists of five samples. It appears unconnected to other clusters.

Cluster: Tyjhu



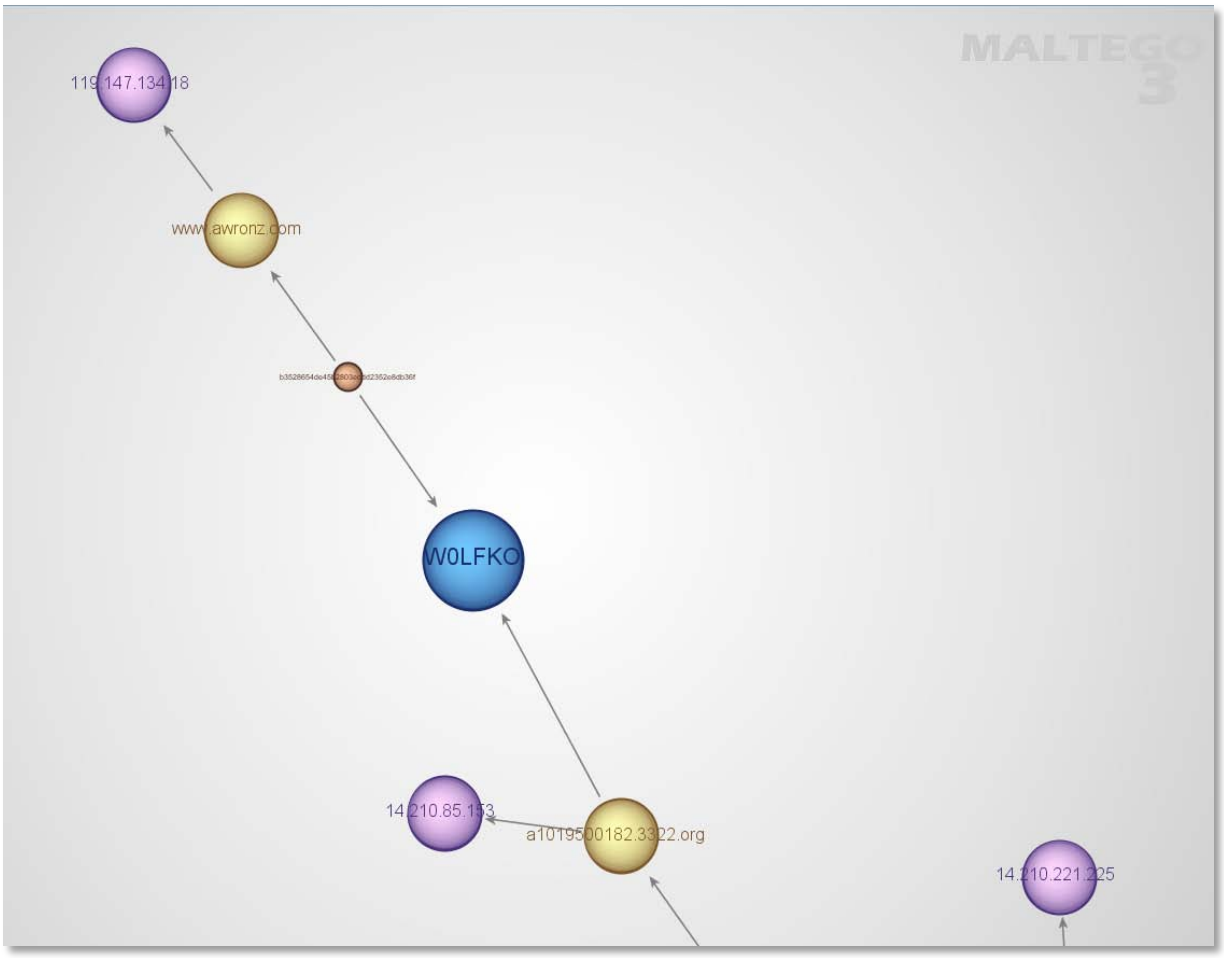
The Tyjhu cluster contains seven samples. It is connected to the Winds cluster through common C&C at troyok.3322.org.

Cluster: URATU

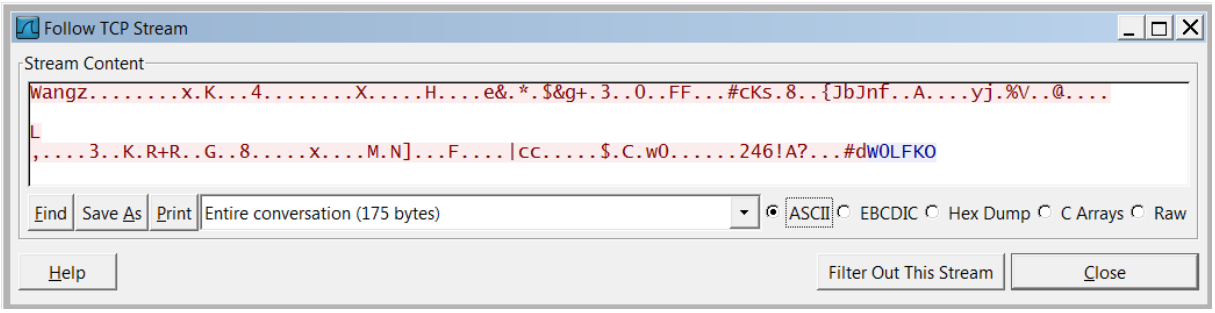


The URATU cluster contains three samples. It appears unconnected with other clusters. However, recently it has been connected with attacks on Nepalese Government websites (12).

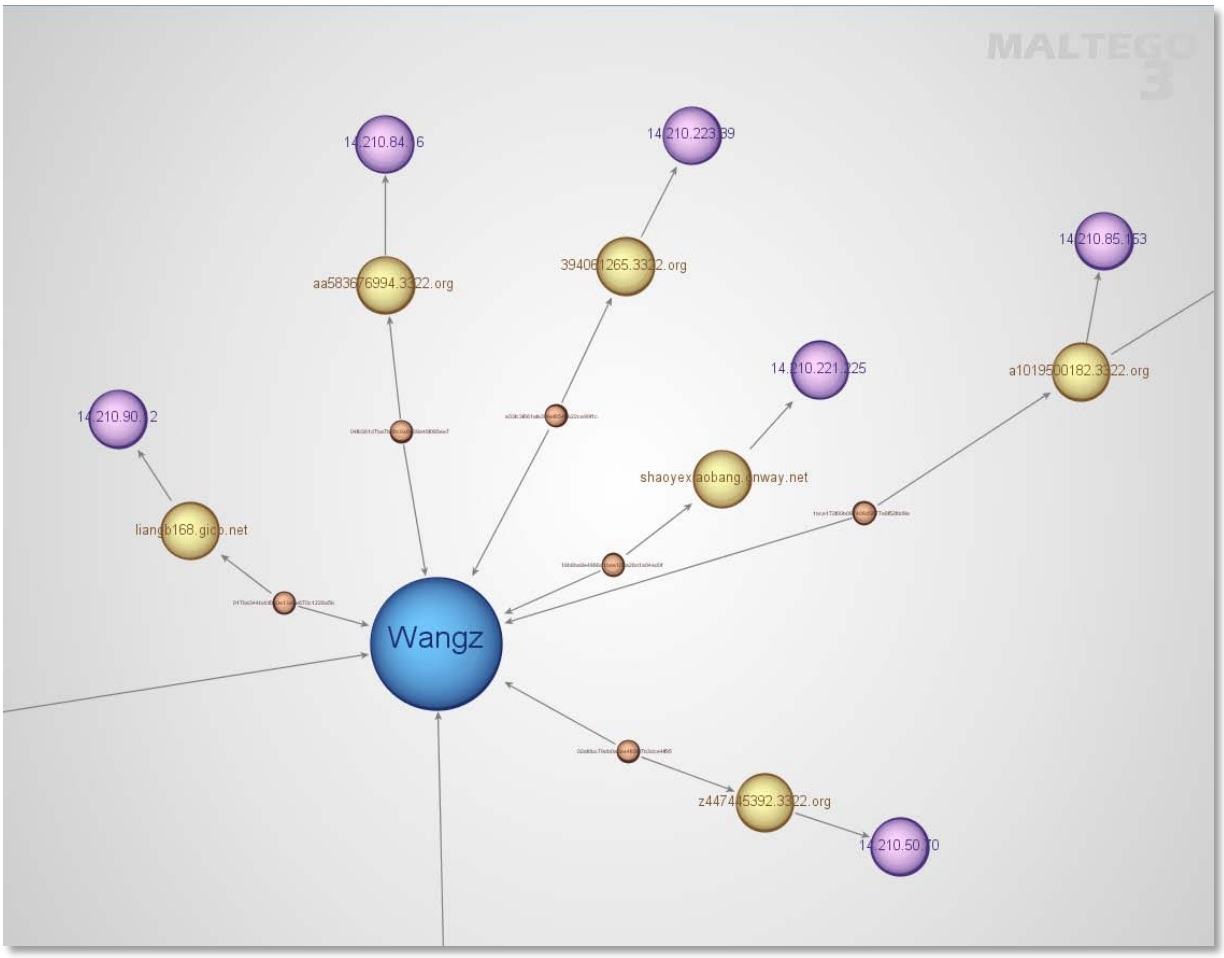
Cluster: W0LFKO



The W0LFKO cluster consists of one sample. It is linked to the Wangz cluster by the C&C a1019500182.3322.org which replies “W0LFKO” when connection is attempted.

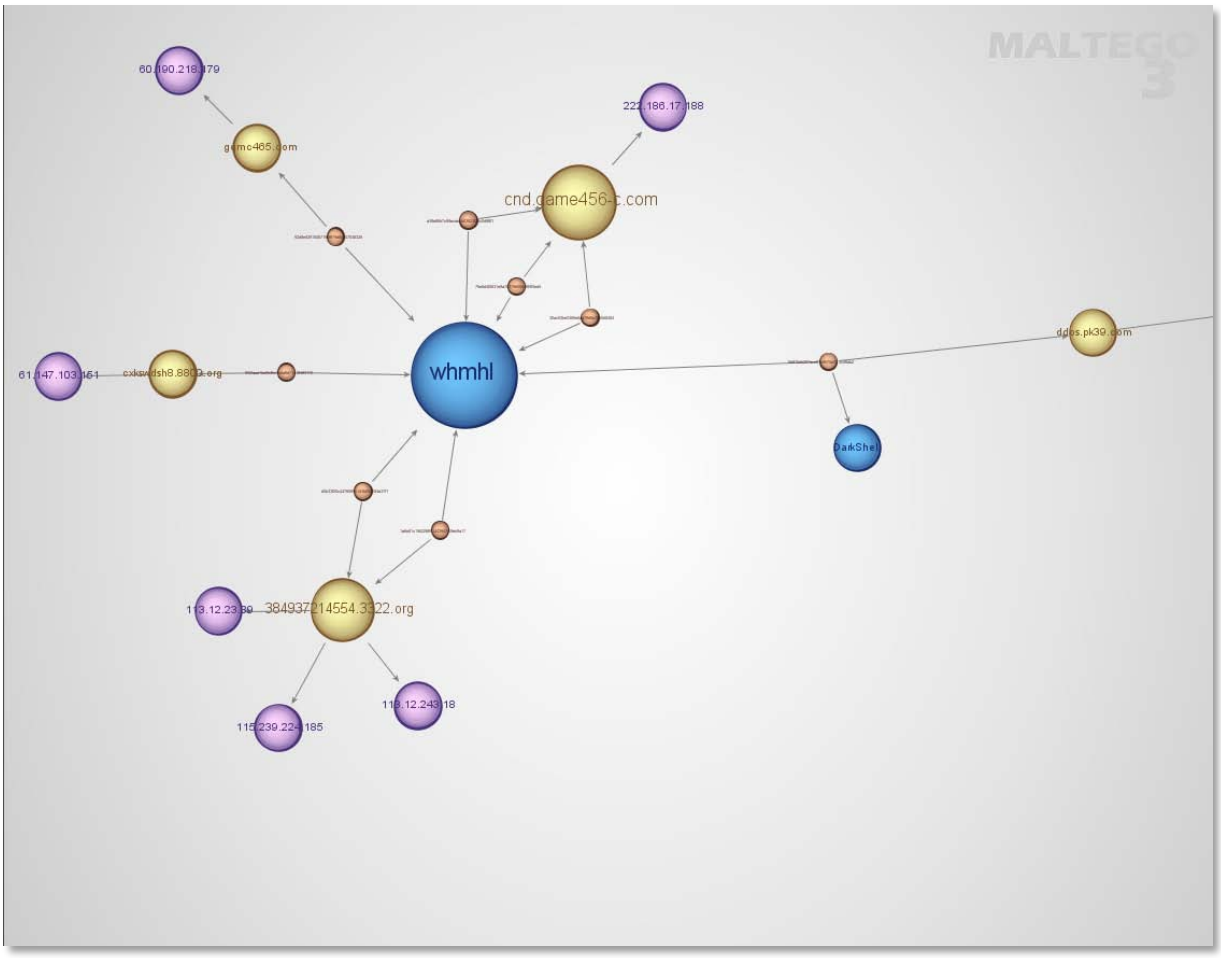


Cluster: Wangz



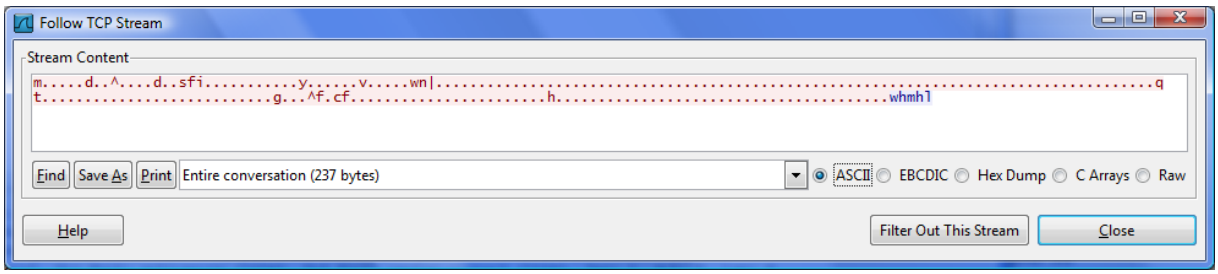
There are eight samples in the Wangz cluster. Wangz links with W0LFKO (see W0LFKO), IM007 (see IM007) clusters, and also with Xjjhi cluster through observed communication from the Wangz C&C a6603892.gicp.net.

Cluster: whmhl

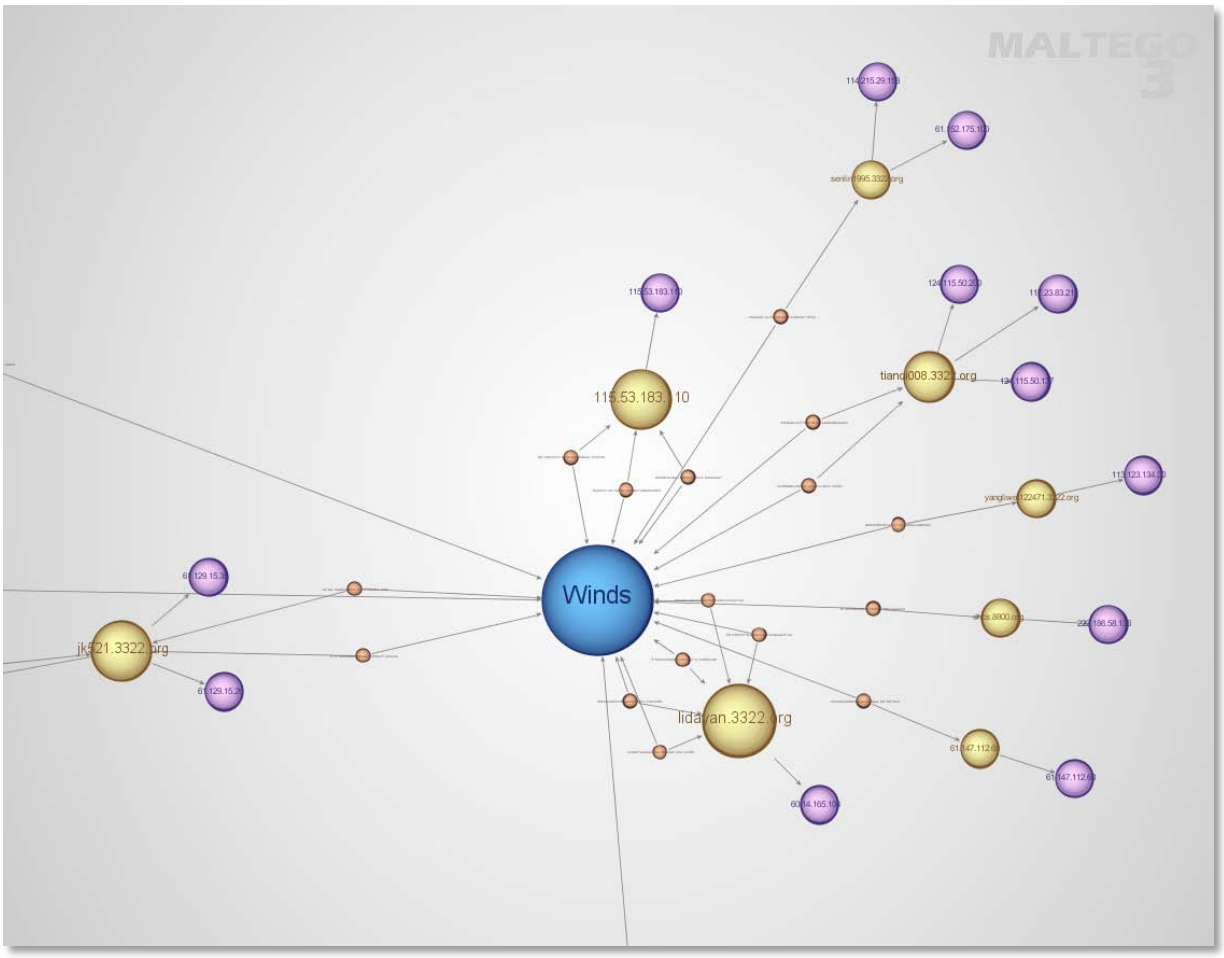


The whmhl cluster consists of 9 samples; actually only 8 are Gh0stRats. The last sample is a DarkShell ddos bot. It is included because it links this cluster with another.

The DarkShell bot connected to ddos.pk39.com on port 5566. This resolved to the same IP as www.pk39.com, the C&C server for the cb1st cluster. The pcap from this connection reveals that ddos.pk39.com replies with “whmhl”. Gotcha.

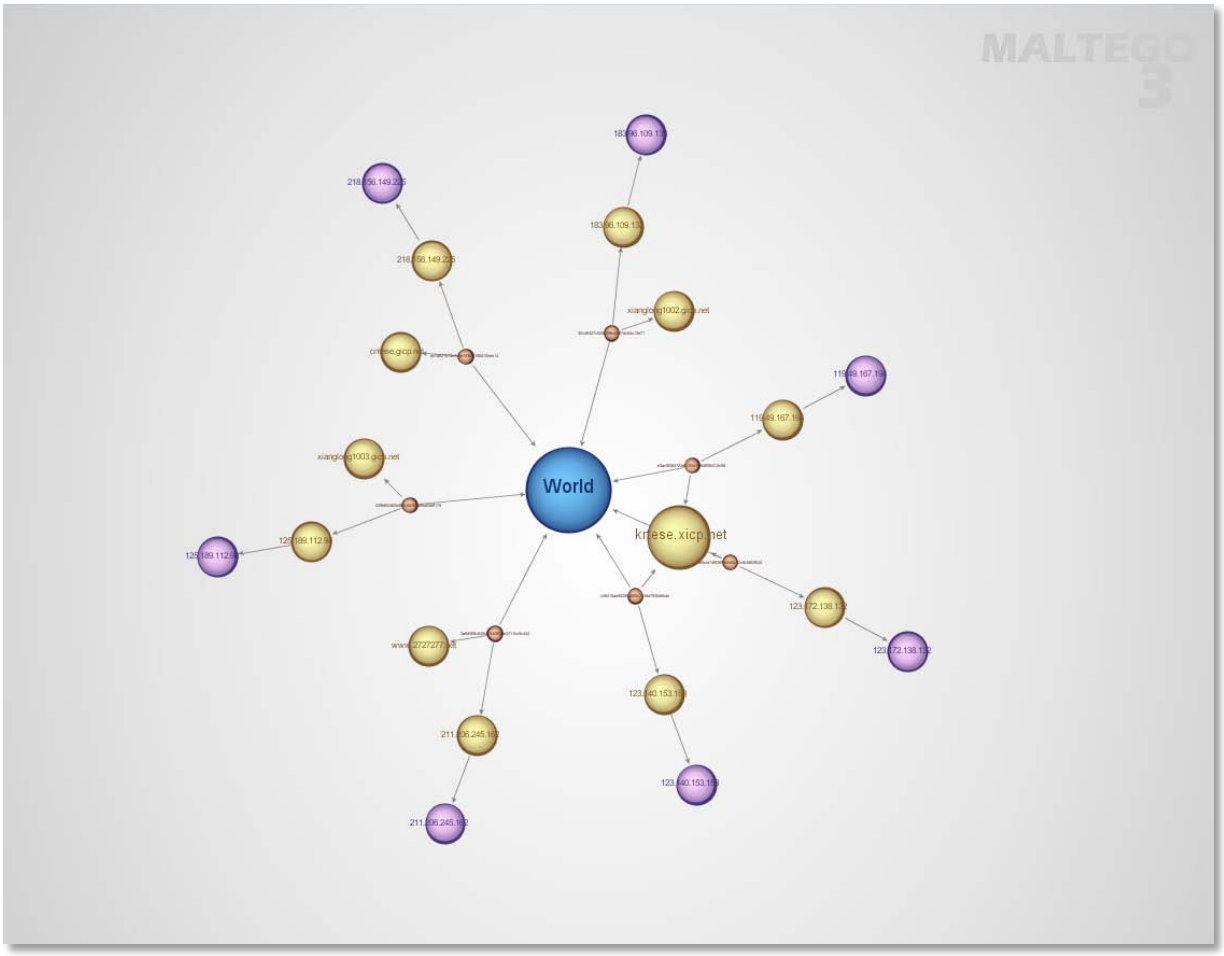


Cluster: Winds



The Winds cluster encompasses 21 samples. It is linked with the Tyjhu cluster (see Tyjhu), the PCRat cluster (see PCRat) and the MoZhe cluster (see MoZhe).

Cluster: World

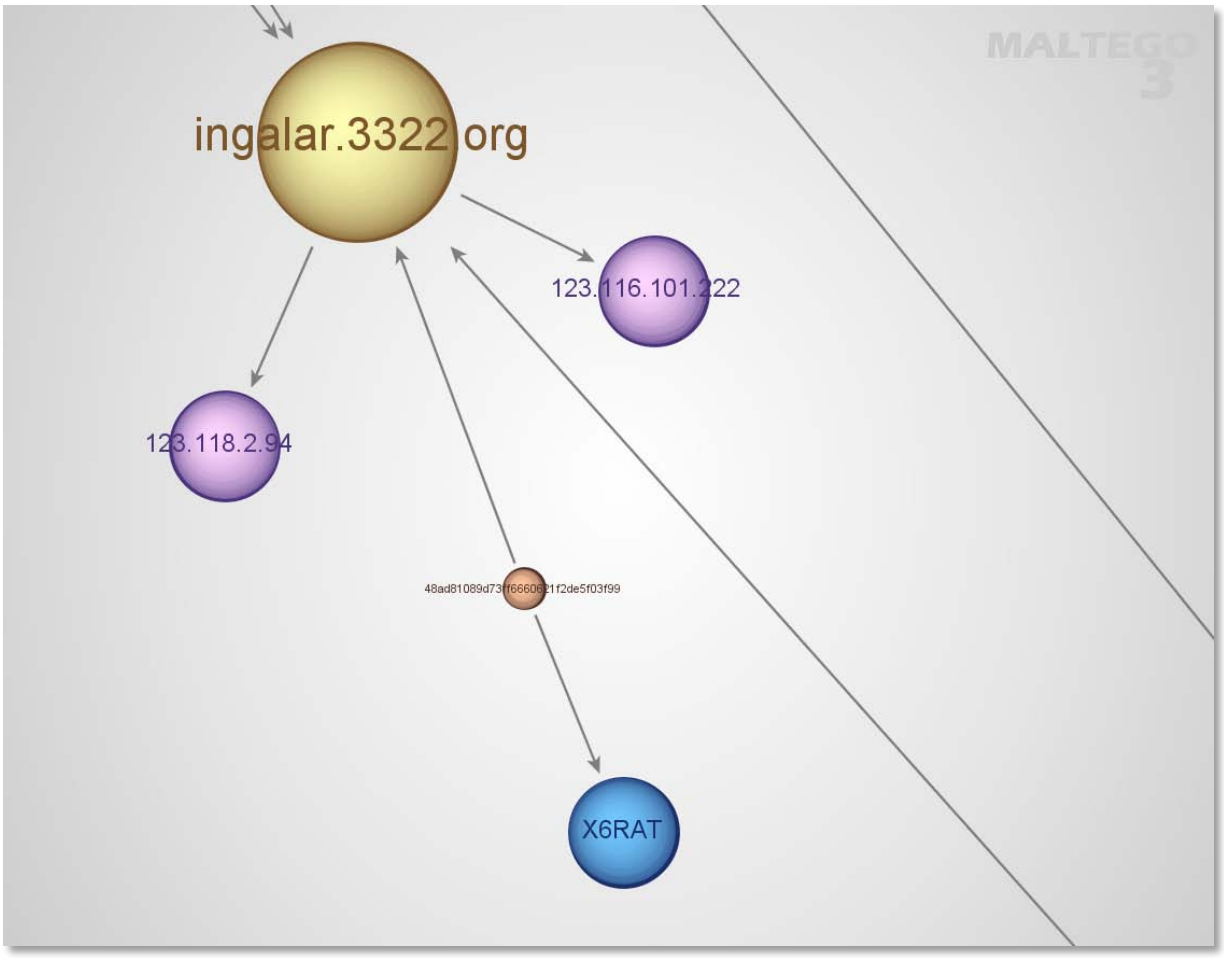


The World cluster consists of seven samples.

Samples in this cluster all give the impression that they use hardcoded IP addresses for their C&C communication. This is because the real C&C ip is not stored in the executable, but exists base64 encoded in a text file downloaded from a remote site. Thus these files are shown with two C&C connections.

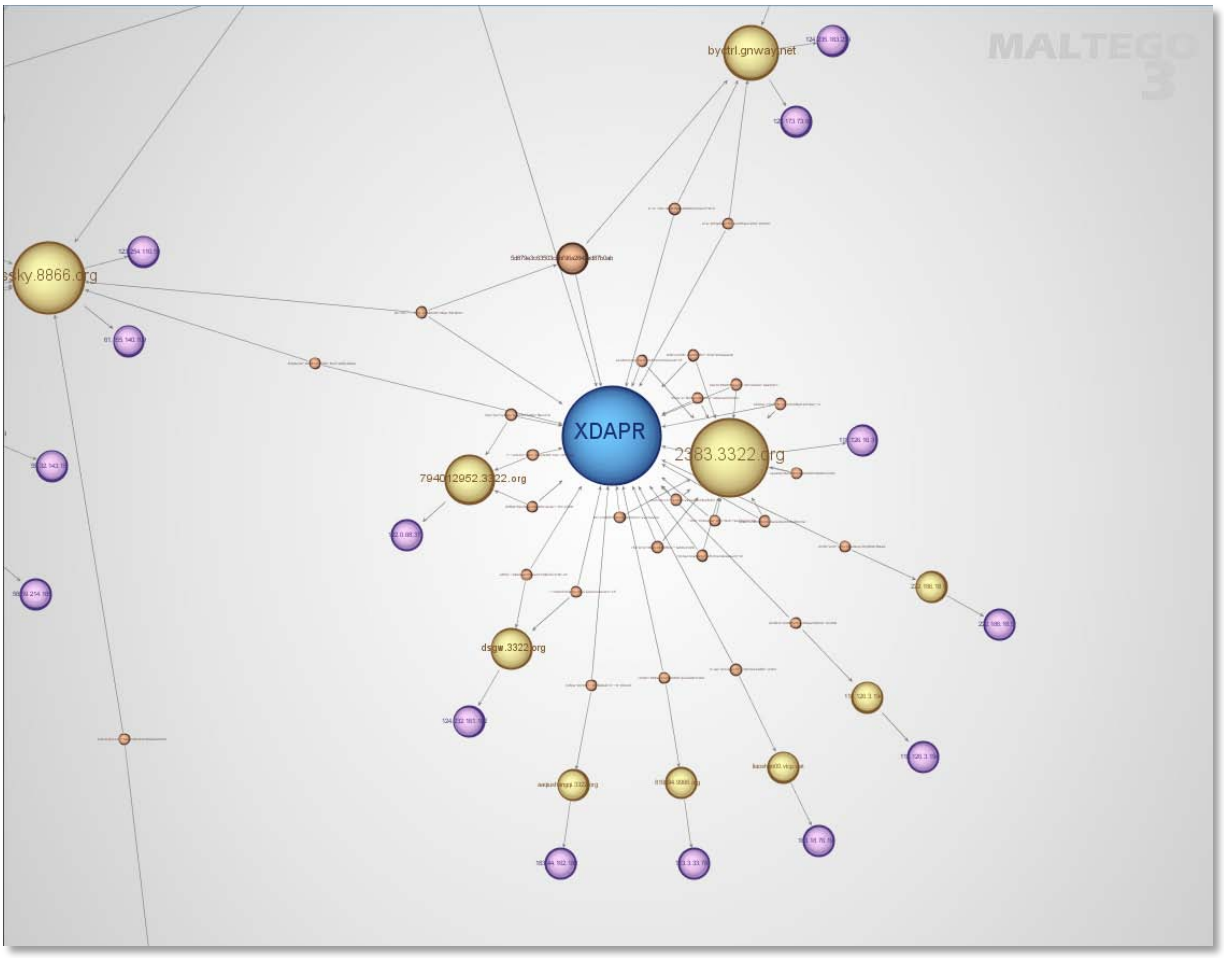
This cluster does not seem linked with other clusters. However, there is a strong resemblance between these samples and some samples in the Wangz cluster (e.g. c577b5a8d07982a2c6c42a7352c0cef8).

Cluster: X6RAT



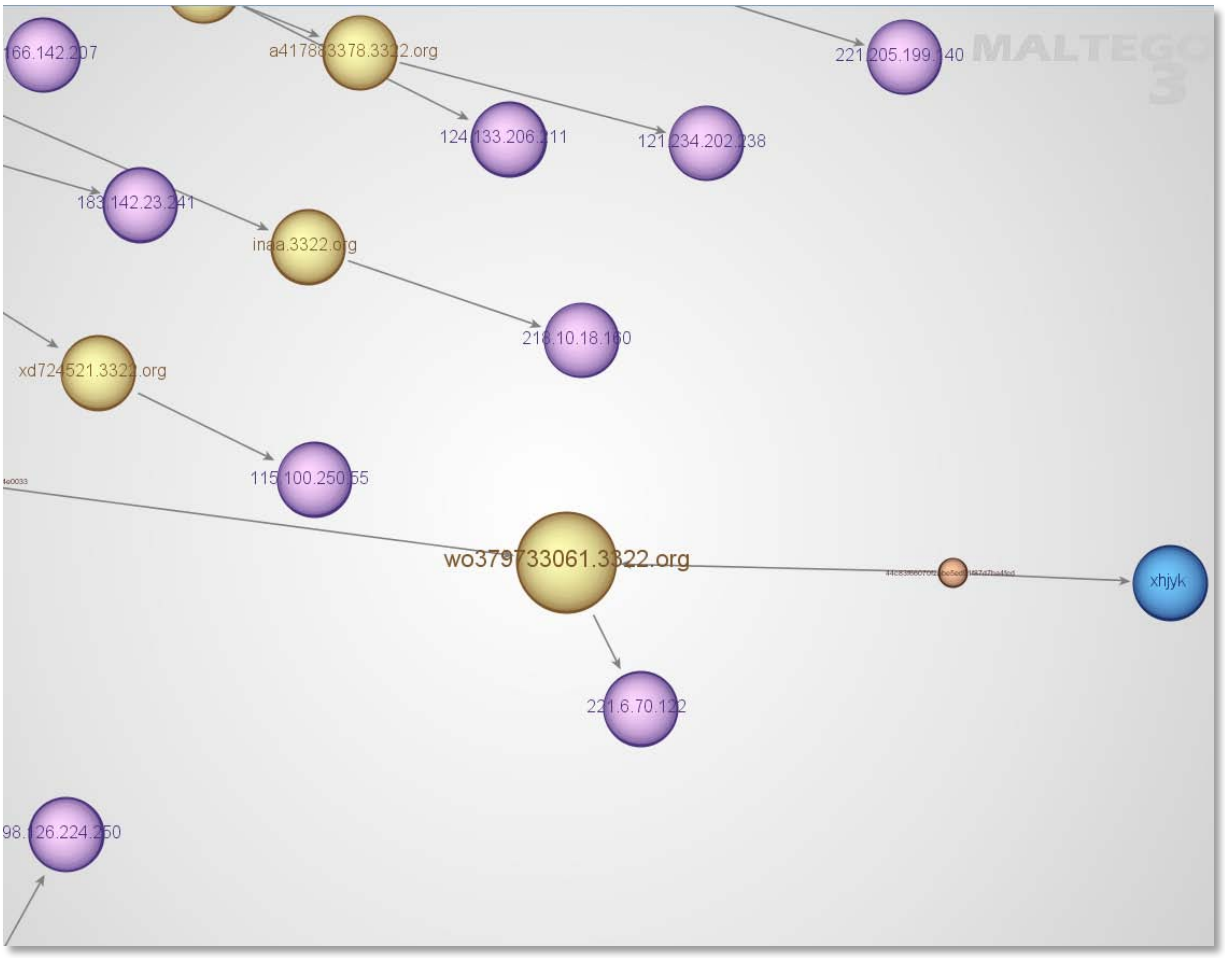
The X6RAT cluster consists of one sample. It is linked to the MoZhe cluster (see MoZhe) and Gh0st.

Cluster: XDAPR



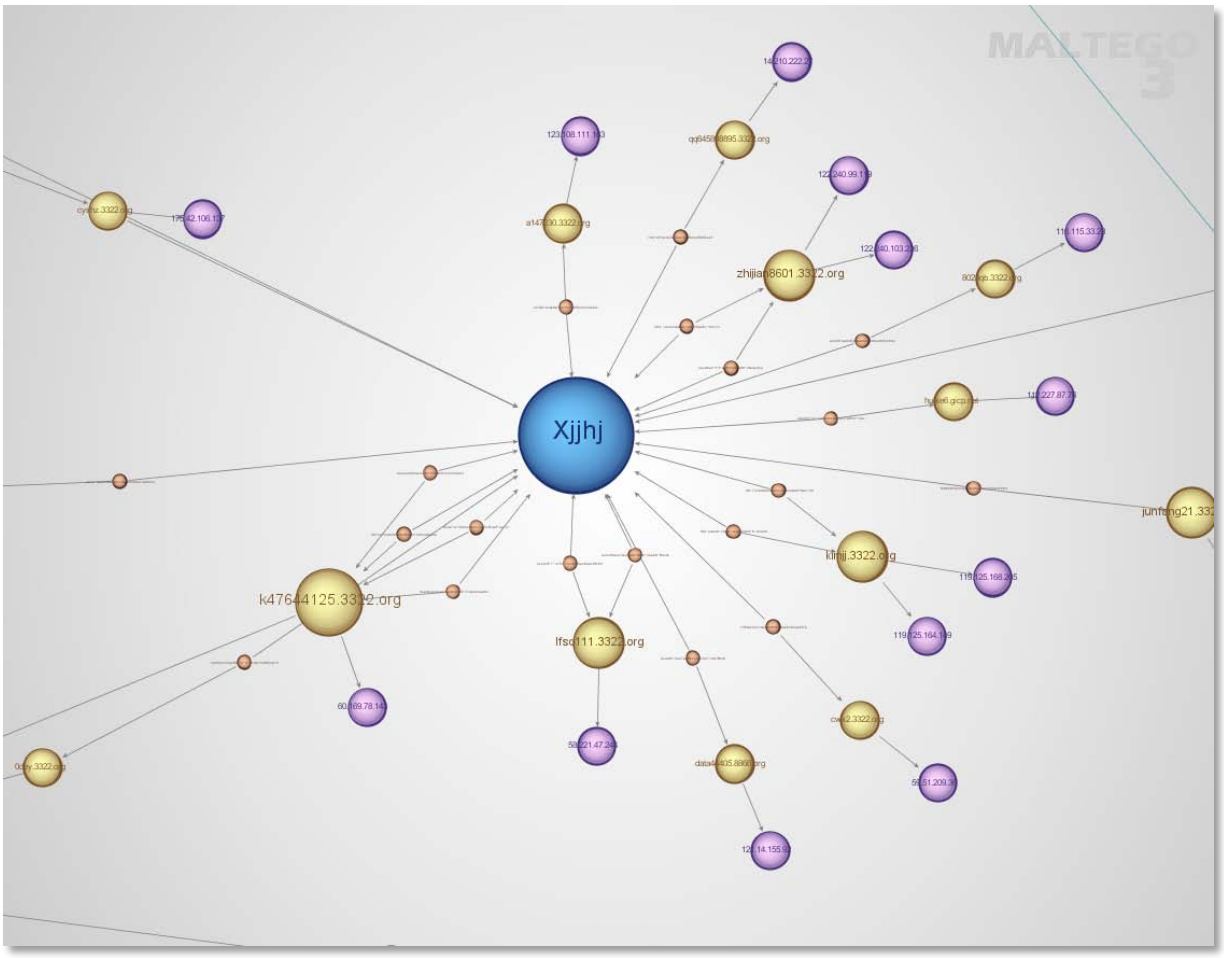
The XDAPR cluster contains 28 samples. It is linked with the KrisR, HXWAN, cb1st, FKJP3 and Lyyyy clusters. (See KrisR).

Cluster: xhjyk



The xhjyk cluster consists of one sample. Its C&C server, wo379733061.3322.org, is used by another sample (MD5 2f463a39c10d507b4295e16b7b4e0033) which also connects to wk1888.com, the C&C for Gh0st and the c1bst clusters. It's also worth noting that one of the C&C's for the KrisR cluster is wo379733063.3322.org – only one digit different from this C&C, and corroborates the impression that the KrisR and cb1st clusters are connected.

Cluster: Xjjhj



The Xjjhj cluster contains 19 samples. It is linked with the Wangz, attac and QWPOT clusters.

Conclusions

This study shows the presence of several logical links between different Ghost campaigns: Links between malware type (in this case illustrated by the network protocol magic tag), links in the C&C infrastructure and to some extent links in the registration information.

Due to the necessary scope limitation, many other links had to remain unexamined. However, the present work shows that some of the most active and prolific malware campaigns share enough connections indicate that the same groups or individuals are involved.

In the cases where we have been able to say something about the entities responsible for the attacks, it seems apparent that the persons involved can be considered career criminals. These are people that have their hand in many different types of online crime, have been doing it for quite some time, and often target victims inside China itself.

Smaller clusters are in many ways more interesting. They are often more difficult to track, as they obviously leave less clues as to who is behind the attack and what the purpose is. Clusters that have been involved in targeted attacks typically belong to these.

References

1. **Wikipedia.** GhostNet. *Wikipedia.* [Online]
http://en.wikipedia.org/wiki/GhostNet.

2. **Clean-MX.** wt1888.com. *Clean-MX domain search.* [Online]
http://support.clean-mx.de/clean-mx/viruses.php?domain=wt1888.com.

3. **Clean-MX**. 81266966.com. *Clean-MX domain search.* [Online]
http://support.clean-mx.de/clean-mx/viruses.php?domain=81266966.com.

4. **beishan.info.** [Online]
http://bbs.beishan.info/thread-849-1-1.html.

5. **cyberpolice.cn.** *Nanchang Cyberpolice.* [Online]
http://www.nanchang.cyberpolice.cn/show_news.asp?ID=1160.

6. **Blasco, Jaime.** Targeted attacks against Tibet organizations. *AlienVault Labs.* [Online]
http://labs.alienvault.com/labs/index.php/2012/targeted-attacks-against-tibet-organizations/.

7. **Villeneuve, Nart.** The Significance of the "Nitro" Attacks. *Trend Micro.* [Online]
http://blog.trendmicro.com/the-significance-of-the-nitro-attacks/.

8. **Command Five Pty Ltd.** Command and Control in the Fifth Domain. [Online]
http://www.commandfive.com/papers/C5_APT_C2InTheFifthDomain.pdf.

9. **University of Toronto.** Recent Observations in Tibet-Related Information Operations: Advanced Social Engineering for the Distribution of LURK Malware. *Citizen Lab.* [Online]
https://citizenlab.org/wp-content/uploads/2012/07/10-2012-recentobservationsintibet.pdf.

10. **Walton, Greg.** Tibetan journalists targeted by Gh0stRAT in Protest pictures.rar. *MalwareLab.* [Online]
https://malwarelab.zendesk.com/entries/21199507-tibetan-journalists-targeted-by-gh0strat-in-protest-pictures-rar.

11. **Blasco, Jaime.** New MaControl variant targeting Uyghur users, the Windows version using Gh0st RAT. *AlienVault Labs.* [Online]
http://labs.alienvault.com/labs/index.php/2012/new-macontrol-variant-targeting-uyghur-users-the-windows-version-using-gh0st-rat/.

12. **Giuliani, Gianluca og Sharf, Elad.** Nepalese government websites compromised to serve Zegost RAT . *Websense Security Labs Blog.* [Online]
http://community.websense.com/blogs/securitylabs/archive/2012/08/08/nepalese-government-websites-compromised-to-serve-zegost-backdoor.aspx.