

# 我们近期看到的针对乌克兰和俄罗斯的DDoS攻击细节

blog.netlab.360.com/wo-men-kan-dao-de-wu-ke-lan-bei-ddosgong-ji-xi-jie/

360Netlab

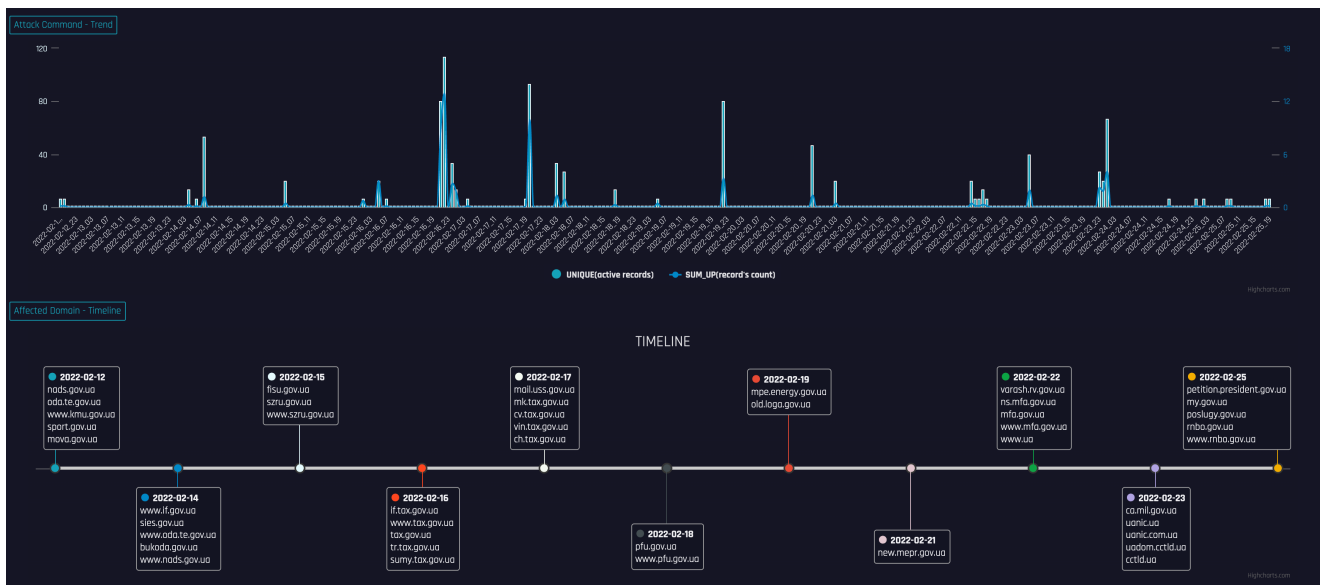
February 25, 2022

25 February 2022 / Botnet

在360Netlab (netlab.360.com)，我们持续的通过我们的 BotMon 系统跟踪全球范围内的僵尸网络。特别的，对于DDoS 相关的僵尸网络，我们会进一步跟踪其内部指令，从而得以了解攻击的细节，包括攻击者是谁、受害者是谁、在什么时间、具体使用什么攻击方式。最近俄乌局势紧张，双方的多个政府、军队和金融机构都遭到了DDoS攻击，我们也不断接收到安全社区的询问，咨询对于最近乌克兰和俄罗斯相关网站 (.ua .ru 下属域名) 遭受DDoS攻击的具体情况，因此我们特意整理相关数据供安全社区参考。

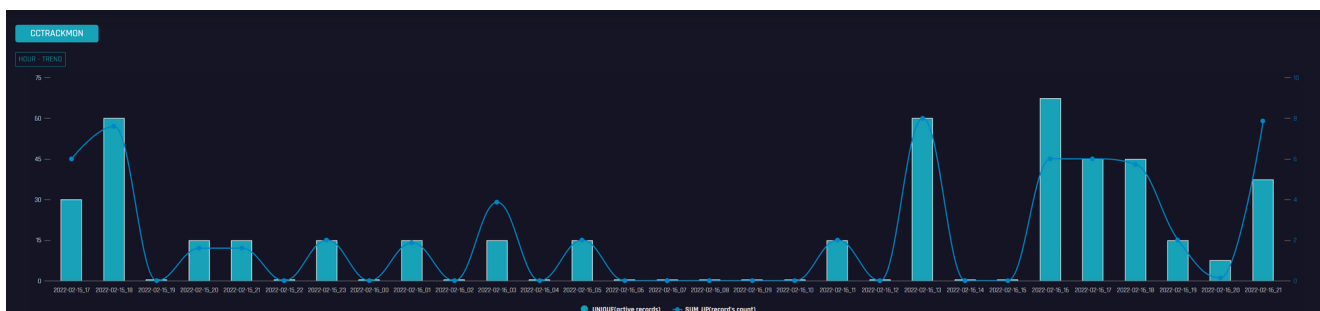
## 针对乌克兰的DDoS攻击

下图是我们看到的针对域名以 .gov.ua 结尾的政府网站的攻击趋势。



可以看到攻击最早始于2月12号，攻击数量和强度都在持续变大，在2月16日达到顶峰，攻击类型则混合了NTP放大、UDP/STD/OVH flood等多种类型

下图是我们看到的针对另一个以 .ua 结尾的网站“online.oschadbank.ua”的DDoS攻击。



可以看到攻击开始自2月15日，持续了3天。值得注意的是攻击这个网站的C2 mirai\_5.182.211.5 2月11号上线，从2022-02-16 03:02:37+08:00发出第一条攻击指令始到2022-02-17 01:08:27+08:00最后一条指令，它只攻击了185.34.x.x/24这个网段的IP，而这些IP均属于“online.oschadbank.ua”。

我们捕获的针对 .ua 网站的DDoS攻击，除了NTP反射放大攻击外，其它的均跟botnet有关，涉及Mirai、Gafgyt、ripprbot、moobot和ircBot等5个家族的10多个C2。因为这些家族业界相关分析已经很多，这里不再赘述，只罗列下我们捕获到的样本和跟踪到的C2指令。除第一个C2自上线以来只用来攻击“oschadbank.ua”相关的几个子站，其他的C2攻击了不同国家的多个目标。限于篇幅，下面罗列首先出现的4个C2。

## 1，mirai\_5.182.211.5

---

前面已经说过，该C2在其活跃期间（2022-02-11~2022-02-17）只攻击了“online.oschadbank.ua”这一个目标。我们的蜜罐从2月11日到2月14日曾持续捕获到它的样本，部分URL和MD5对应如下：

```
e5822f8f9bc541e696f5520b9ad0e627
http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.i486
39532b27e2dbd9af85f2da7ff4519467
http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.mpsl
69b51b792b1fca9a268ce7cc1e1857df
http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.mips
70aaa4746150eba8439308096b17d8cc
http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.arm
68ed4532bd6ad79f263715036dee6021
http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.m68k
54bd85b40041ba82ae1b57664ee3e958
http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.arc
1b7247a2049da033a94375054829335d
http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.i686
ac4d8d0010775e185e12604c0e304685
http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.x86_64
0eca53a2dca6384b7b1b7de186e835b5
http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.sh4
cc79916e1e472a657a9ae216b2602a7b
http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.arm5
8f488f3218baec8b75dc6e42e5c90a47
http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.arm6
b307dd0043e94400f8632c4d0c4eae0e
http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.arm7
340255b25edf28c8de140f3f00306773
http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.spc
e2b103a3b74dd0bfd98ffd27ed07f2c6
http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.x86
```

样本为Mirai变种，具有较强的Mirai代码特征，保留了table\_init()、attack\_init()等典型的Mirai函数。下面是我们跟踪到的指令：

```

2022-02-16 21:27:44+08:00      mirai      5.182.211.5      60195
ddos      atk_7      185.34.224.121
atk_time=600,netmask=32,/wb/api/v2/session,post,
{login:rrre,password:vvv,captcha:},443,online.oschadbank.ua,affected=online.oschadbank

2022-02-16 21:19:04+08:00      mirai      5.182.211.5      60195
ddos      atk_7      185.34.224.121
atk_time=600,netmask=32,online.oschadbank.ua,/wb/api/v2/session,post,
{login:rrre,password:vvv,captcha:}

2022-02-16 21:06:14+08:00      mirai      5.182.211.5      60195
ddos      atk_5      185.34.224.121
atk_time=600,netmask=32,109.110.75.23,443,1,1,1,affected=online.oschadbank.ua

2022-02-16 19:17:12+08:00      mirai      5.182.211.5      60195
ddos      atk_5      185.34.224.121
atk_time=1200,netmask=32,1,109.254.6.88,443,1,1,affected=online.oschadbank.ua

2022-02-16 18:55:07+08:00      mirai      5.182.211.5      60195
ddos      atk_5      185.34.224.121
atk_time=1200,netmask=32,1,93.188.39.70,443,1,1,affected=online.oschadbank.ua

2022-02-16 18:34:18+08:00      mirai      5.182.211.5      60195
ddos      atk_5      185.34.224.121
atk_time=1200,netmask=32,91.206.111.88,443,1,1,1,affected=online.oschadbank.ua

2022-02-16 18:15:23+08:00      mirai      5.182.211.5      60195
ddos      atk_5      185.34.224.121
atk_time=1200,netmask=32,78.26.168.101,443,1,1,1,affected=online.oschadbank.ua

2022-02-16 17:55:35+08:00      mirai      5.182.211.5      60195
ddos      atk_5      185.34.224.121
atk_time=1200,netmask=32,195.182.202.20,443,1,1,1,affected=online.oschadbank.ua

2022-02-16 17:39:01+08:00      mirai      5.182.211.5      60195
ddos      atk_5      185.34.224.121
atk_time=900,netmask=32,443,1,1,1,37.115.24.108,affected=online.oschadbank.ua

2022-02-16 17:24:37+08:00      mirai      5.182.211.5      60195
ddos      atk_5      185.34.224.121
atk_time=900,netmask=32,78.31.254.20,443,1,1,1,affected=online.oschadbank.ua

2022-02-16 17:24:37+08:00      mirai      5.182.211.5      60195
ddos      atk_5      185.34.224.121
atk_time=900,netmask=32,78.31.254.20,443,1,1,1,affected=online.oschadbank.ua

2022-02-16 16:48:55+08:00      mirai      5.182.211.5      60195
ddos      atk_5      185.34.224.121
atk_time=900,netmask=32,443,1,1,1,249,46.219.126.90,affected=online.oschadbank.ua

2022-02-16 13:41:41+08:00      mirai      5.182.211.5      60195
ddos      atk_5      185.34.224.121
atk_time=120,netmask=32,255.255.255.255,443,1,affected=online.oschadbank.ua

2022-02-16 13:25:49+08:00      mirai      5.182.211.5      60195
ddos      atk_5      185.34.224.121
atk_time=120,netmask=32,255.255.255.255,443,1,affected=online.oschadbank.ua

2022-02-16 13:23:33+08:00      mirai      5.182.211.5      60195
ddos      atk_6      185.34.224.121
atk_time=120,netmask=32,255.255.255.255,443,affected=online.oschadbank.ua

2022-02-16 11:06:32+08:00      mirai      5.182.211.5      60195
ddos      atk_5      185.34.224.121
atk_time=10800,netmask=32,255.255.255.255,443,affected=online.oschadbank.ua

2022-02-16 05:04:45+08:00      mirai      5.182.211.5      60195
ddos      atk_5      185.34.224.121
atk_time=21600,netmask=32,255.255.255.255,443,affected=online.oschadbank.ua

2022-02-16 01:02:32+08:00      mirai      5.182.211.5      60195

```

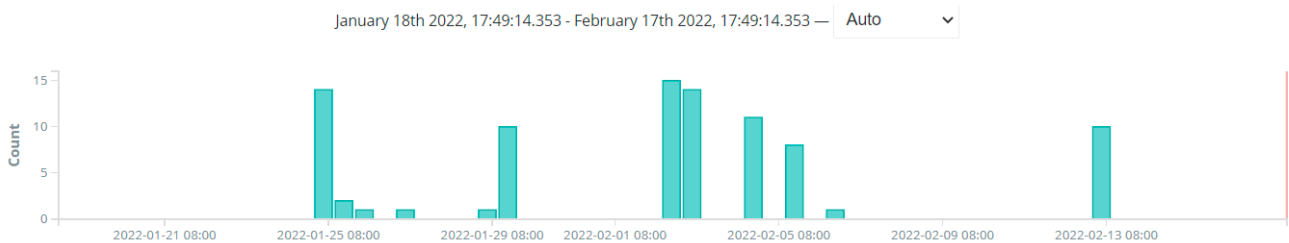
```

ddos      atk_5      185.34.224.121
atk_time=7200,netmask=32,255.255.255.255,443,affected=online.oschadbank.ua
2022-02-15 23:00:06+08:00      mirai      5.182.211.5      60195
ddos      atk_5      185.34.224.121
atk_time=7200,netmask=32,255.255.255.255,443,affected=online.oschadbank.ua
2022-02-15 21:00:08+08:00      mirai      5.182.211.5      60195
ddos      atk_5      185.34.224.121
atk_time=7200,netmask=32,255.255.255.255,443,affected=online.oschadbank.ua
2022-02-15 20:01:13+08:00      mirai      5.182.211.5      60195
ddos      atk_5      185.34.224.121
atk_time=3600,netmask=32,255.255.255.255,443,affected=online.oschadbank.ua
2022-02-15 18:55:36+08:00      mirai      5.182.211.5      60195
ddos      atk_5      185.34.224.121
atk_time=3600,netmask=32,255.255.255.255,443,affected=online.oschadbank.ua
2022-02-15 18:30:32+08:00      mirai      5.182.211.5      60195
ddos      atk_5      185.34.224.121
atk_time=1800,netmask=32,255.255.255.255,443,affected=online.oschadbank.ua
2022-02-15 18:08:50+08:00      mirai      5.182.211.5      60195
ddos      atk_0      185.34.224.121
atk_time=600,netmask=32,,affected=online.oschadbank.ua
2022-02-15 17:42:26+08:00      mirai      5.182.211.5      60195
ddos      atk_7      185.34.224.121
atk_time=600,netmask=32,online.oschadbank.ua,affected=online.oschadbank.ua

```

## 2 , mirai\_209.141.33.208

该C2的样本1月25日便已经出现，样本捕获情况如下图所示。



它在16日攻击了“www.szru.gov.ua”网站：

```

2022-02-16 05:35:38+08:00      mirai      209.141.33.208
209.141.33.208 9999      atk_2      193.109.8.66      80
{'netmask': 32,'flags': [{'fid': 7,'value': b'80'}]},affected=www.szru.gov.ua

```

## 3 , gafgyt\_172.245.6.134

该C2的样本最早1月29日开始传播，样本捕获情况如下图所示。



下面是我们跟踪到的指令：

2022-02-17 01:46:30+08:00	gafgyt	172.245.6.134	61108
ddos	OVH	213.156.91.92	
uri=/,OVH,213.156.91.92,443,30,1024,affected=mail.uss.gov.ua			
2022-02-17 00:08:31+08:00	gafgyt	172.245.6.134	61108
ddos	OVH	193.17.44.246	
uri=/,OVH,193.17.44.246,443,60,1024,affected=bank.gov.ua			
2022-02-17 00:07:40+08:00	gafgyt	172.245.6.134	61108
ddos	HEX	193.17.44.146	
uri=/,HEX,193.17.44.146,443,60,affected=bank.gov.ua			
2022-02-16 22:19:04+08:00	gafgyt	172.245.6.134	61108
ddos	OVH	193.17.44.246	
uri=/,OVH,193.17.44.246,443,200,1024,affected=bank.gov.ua			
2022-02-16 22:18:33+08:00	gafgyt	172.245.6.134	61108
ddos	OVH	193.17.44.146	
uri=/,OVH,193.17.44.146,443,200,1024,affected=bank.gov.ua			
2022-02-16 22:07:34+08:00	gafgyt	172.245.6.134	61108
ddos	HEX	193.109.8.66	
uri=/,HEX,193.109.8.66,80,60,affected=www.szru.gov.ua			
2022-02-16 22:01:44+08:00	gafgyt	172.245.6.134	61108
ddos	HEX	193.17.44.146	
uri=/,HEX,193.17.44.146,80,30,1024,affected=bank.gov.ua			
2022-02-16 21:57:02+08:00	gafgyt	172.245.6.134	61108
ddos	OVH	193.17.44.246	
uri=/,OVH,193.17.44.246,443,60,1024,affected=bank.gov.ua			
2022-02-16 21:53:16+08:00	gafgyt	172.245.6.134	61108
ddos	OVH	193.17.44.246	
uri=/,OVH,193.17.44.246,443,60,1024,affected=bank.gov.ua			
2022-02-16 21:46:41+08:00	gafgyt	172.245.6.134	61108
ddos	HEX	193.29.204.11	
uri=/,HEX,193.29.204.11,443,120,affected=www.president.gov.ua			
2022-02-16 21:44:41+08:00	gafgyt	172.245.6.134	61108
ddos	HEX	195.78.68.7	
uri=/,HEX,195.78.68.7,80,120,affected=mova-ombudsman.gov.ua			
2022-02-16 05:35:27+08:00	gafgyt	172.245.6.134	61108
ddos	HEX	193.109.8.66	
uri=/,HEX,193.109.8.66,80,20,affected=fisu.gov.ua			

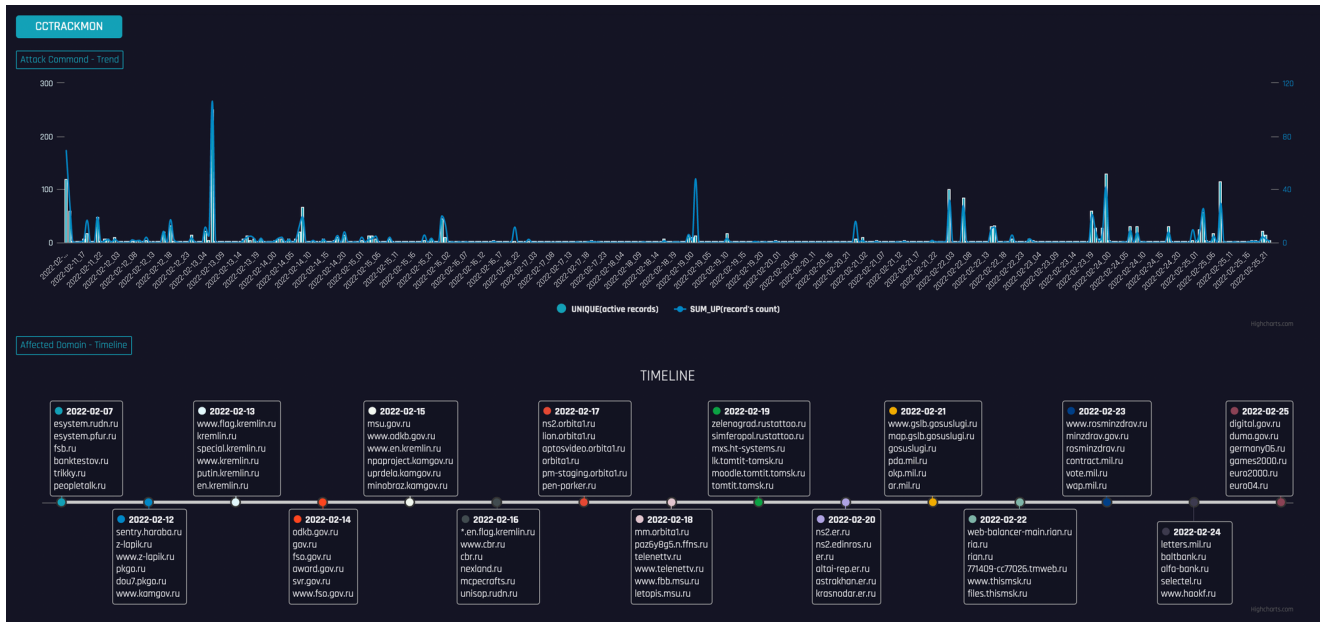
#### 4 , gafgyt\_188.127.237.5

该C2的样本在2月6日被捕获，它在2月16日攻击了“od.tax.gov.ua”网站：

2022-02-16 01:54:00+08:00	gafgyt	188.127.237.5	606
STDHEX	193.200.32.26	STDHEX,193.200.32.	
26,80,120,affected=od.tax.gov.ua			

#### 针对俄罗斯的DDoS攻击

下图是我们看到的针对以 .ru 结尾的俄罗斯政府和军队网站的攻击。



可以看到，针对俄国的DDoS攻击从2月7日就开始了，持续至今且数量呈增加趋势。跟乌克兰相比，针对俄国的DDoS攻击其实更多，限于篇幅，下面只罗列涉事botnet的C2。

```

gafgyt_195.133.40.71
gafgyt_212.192.241.44
gafgyt_46.249.32.109
mirai_130.162.32.102
mirai_137.74.155.78
mirai_142.93.125.122
mirai_152.89.239.12
mirai_173.254.204.124
mirai_185.245.96.227
mirai_45.61.136.130
mirai_45.61.186.13
mirai_46.29.166.105
mirai_84.201.154.133
mirai_ardp.hldns.ru
mirai_aurora_life.zerobytes.cc
mirai_cherry.1337.cx
mirai_offshore.us.to
mirai_pear.1337.cx
mirai_wpcservice.hldns.ru
moobot_185.224.129.233
moobot_goodpackets.cc
riprbot_171.22.109.201
riprbot_212.192.246.183
riprbot_212.192.246.186

```

## IoC

# C2 mirai\_5.182.211.5  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.arc  
54bd85b40041ba82ae1b57664ee3e958  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.arm  
5096be3bab6b9731293472d7cbd78d18  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.arm  
70aaa4746150eba8439308096b17d8cc  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.arm5  
9636a88f8543b35d212e240c3094d7bb  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.arm5  
cc79916e1e472a657a9ae216b2602a7b  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.arm6  
8f488f3218baec8b75dc6e42e5c90a47  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.arm6  
c5350546e6d22075ac58f0b4410a9c9a  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.arm7  
59b9988a7132fda4fb89b3758411e9df  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.arm7  
b307dd0043e94400f8632c4d0c4eae0e  
# hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.i486  
49b9d14010071605549dc0dfb77d5f59  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.i486  
e5822f8f9bc541e696f5520b9ad0e627  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.i686  
1b7247a2049da033a94375054829335d  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.i686  
c2135973f6d059d9dd09a853cfa241fc  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.m68k  
45677381938006bbc019753dfdfb945  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.m68k  
68ed4532bd6ad79f263715036dee6021  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.mips  
69b51b792b1fca9a268ce7cc1e1857df  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.mips  
d38cc4879fe0bc66cb8e772b28fbfd15  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.mps1  
39532b27e2dbd9af85f2da7ff4519467  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.mps1  
69717fbd6954f16794ff46e4b7c0f58a  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.ppc  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.sh4  
0eca53a2dca6384b7b1b7de186e835b5  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.sh4  
b21e118e9f6b4b393719e0669214946a  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.spc  
340255b25edf28c8de140f3f00306773  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.spc  
84c7c39e3f1a4bdfdcfaa4800d410829  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.x86  
bfaffefb3cc7f301d017242ca832cf45  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.x86  
e2b103a3b74dd0bfd98ffd27ed07f2c6  
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.x86\_64  
8be8a51819d7493de15c5ad7471fe1cc

```
# C2 mirai_209.141.33.208
hxxp://209.141.33.208/bins/Zeus.arm          ac9a7a24b3e5229df0e35f99bd8f4dd0
hxxp://209.141.33.208/bins/Zeus.arm5       0592fc8590bb8b01618bd1075bf45971
hxxp://209.141.33.208/bins/Zeus.arm6       a9a286065f59e833ce6310e4ca0a327a
hxxp://209.141.33.208/bins/Zeus.arm7       2a9ad76fbfe573820d89edc832a759a9
hxxp://209.141.33.208/bins/Zeus.m68k      16cc3f8359b55d32f133ecfd78092dcd
hxxp://209.141.33.208/bins/Zeus.mips      75011d511ee19c482cd12271c238d7d3
hxxp://209.141.33.208/bins/Zeus.mpsl      f3dd9da090cc830e370dfa3a96128bd0
hxxp://209.141.33.208/bins/Zeus.ppc       a7578b554b50cf01c43ebc54c3029fb2
hxxp://209.141.33.208/bins/Zeus.sh4       9798c9f24407da3bb709384f161e20a5
hxxp://209.141.33.208/bins/Zeus.spc       283d7df13561c851d8959f24dce2af99
hxxp://209.141.33.208/bins/Zeus.x86       d1bf7c6e6dde347ea3414cbf38b4e25f
```

```
# C2 gafgyt_172.245.6.134
hxxp://172.245.6.134:80/bins/arc           ed6013177b8c7e61f936c14b698c7bdc
hxxp://172.245.6.134:80/bins/arm         89bb874db266e9aa4d9c07e994a0f02d
hxxp://172.245.6.134:80/bins/arm5       6a9587b5c95d16ce915c3218aa0ef68c
hxxp://172.245.6.134:80/bins/arm6       53526f9affd4d2219e6a33d497ef17f3
hxxp://172.245.6.134:80/bins/arm7       831353dd99cae5bb9ae7dcf125bbe46c
hxxp://172.245.6.134:80/bins/m68k      ad59c219813642fc8d9af23131db12d1
hxxp://172.245.6.134:80/bins/mips      72e13614d7f45adce589d3ab6a855653
hxxp://172.245.6.134:80/bins/mpsl      9d2ed5fb9b586cb369b63aea5ee9c49e
hxxp://172.245.6.134:80/bins/ppc       4b0b53b2f13ceb16b14f8cf7596682bc
hxxp://172.245.6.134:80/bins/sh4       8e26db0a91c6cc2c410764d1f32bbac3
hxxp://172.245.6.134:80/bins/spc       13ead0d75d2fcd53c7d6d8f40f615f4
hxxp://172.245.6.134:80/bins/x86       015ed26cc1656246177004eab5c059fe
hxxp://172.245.6.134:80/bins/x86       67d2f13fcd2622c85d974a6c41c285a4
```

```
# C2: gafgyt_188.127.237.5
hxxp://188.127.237.5/a-r.m-4.Sakura      f422e76ceead6fb12a1c53a68ed2f554
hxxp://188.127.237.5/a-r.m-5.Sakura      870e6969eb7db126e945cfd7e9a2ed5f
hxxp://188.127.237.5/a-r.m-6.Sakura      619517a7ff244de1dc574d2fffb6553d3
hxxp://188.127.237.5/a-r.m-7.Sakura      478ab4262768222839d51c7ea2e5e46f
hxxp://188.127.237.5/i-5.8-6.Sakura      03f6aeda4b403cead904240faec8d32f
hxxp://188.127.237.5/m-6.8-k.Sakura      d3dd19a2ae9228ca71bdf58e3450e205
hxxp://188.127.237.5/m-i.p-s.Sakura      2a2cc9b33cfefc1f8dcf4eed09666ddc
hxxp://188.127.237.5/m-p.s-l.Sakura      37f0100946589aeacdc647ccb14e9baa
hxxp://188.127.237.5/p-p.c-.Sakura      f422e76ceead6fb12a1c53a68ed2f554
hxxp://188.127.237.5/s-h.4-.Sakura      df831e3d07da42cfa5acf95ef97a753a
hxxp://188.127.237.5/x-3.2-.Sakura      8c2a26b9171964d12739addb750f2782
hxxp://188.127.237.5/x-8.6-.Sakura      9612862c128b5df388258a2e76e811a0
```

其它攻击过.ru网站的C2:

```
gafgyt_195.133.40.71
gafgyt_212.192.241.44
gafgyt_46.249.32.109
mirai_130.162.32.102
mirai_137.74.155.78
mirai_142.93.125.122
mirai_152.89.239.12
mirai_173.254.204.124
mirai_185.245.96.227
mirai_45.61.136.130
mirai_45.61.186.13
```



mirai\_46.29.166.105  
mirai\_84.201.154.133  
mirai\_ardp.hldns.ru  
mirai\_aurora\_life.zerobytes.cc  
mirai\_cherry.1337.cx  
mirai\_offshore.us.to  
mirai\_pear.1337.cx  
mirai\_wpceservice.hldns.ru  
moobot\_185.224.129.233  
moobot\_goodpackets.cc  
riprrbot\_171.22.109.201  
riprrbot\_212.192.246.183  
riprrbot\_212.192.246.186