DDoS

Some details of the DDoS attacks targeting Ukraine and Russia in recent days

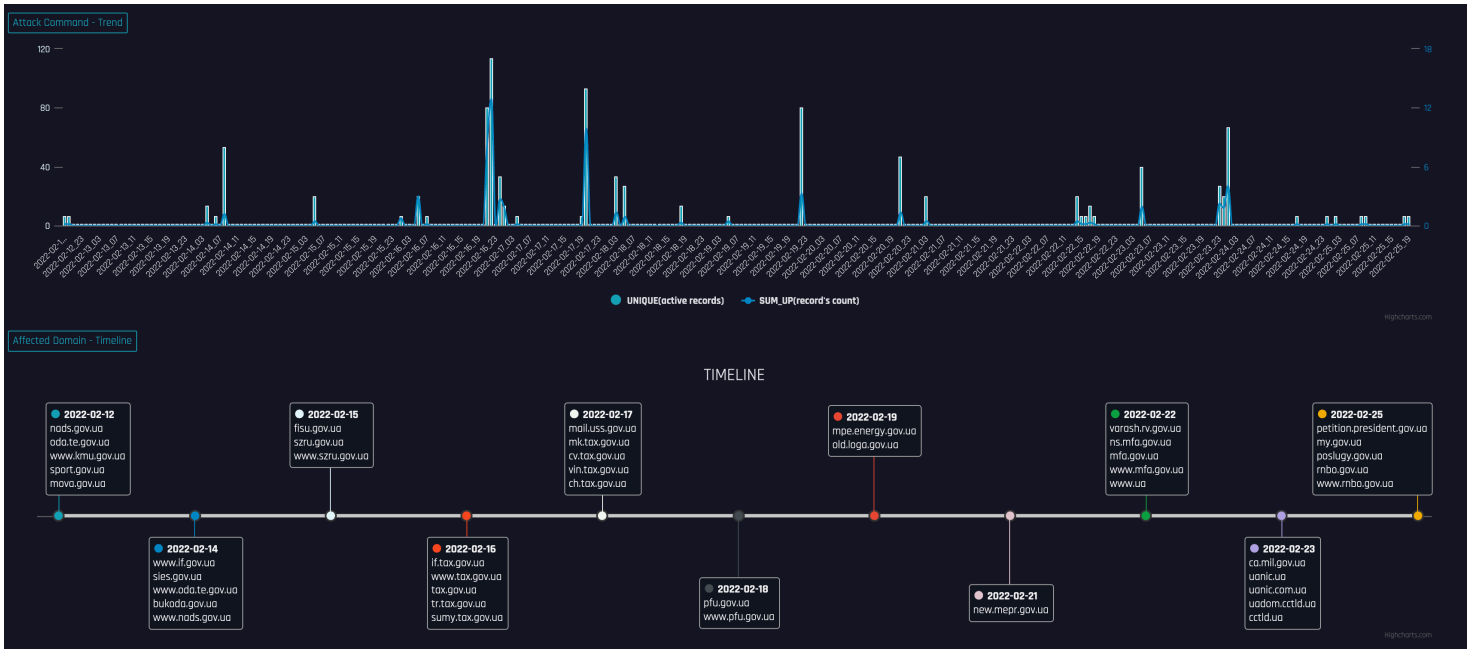
360Netlab
Feb 25, 2022 • 11 min read

At 360Netlab, we continuously track botnets on a global scale through our BotMon system. In particular, for DDoS-related botnets, we further tap into their C2 communications to enable us really see the details of the attacks. Equipped with this visibility, when attack happens, we can have a clear picture of who the victim is, when, and exactly how the attack is carried out.

With the recent tensions between Russia and Ukraine, various government, military and financial institutions on both sides have been DDoSed. We have received inquiries from multiple channels about the specifics of the recent DDoS attacks on Ukrainian and Russian related websites, if we want a comprehensive and thorough analysis, there are tons of data still need to be combed through, this blog is only written to give our readers some quick updates, depends on the situation, we might have more in-depth ones to follow up.

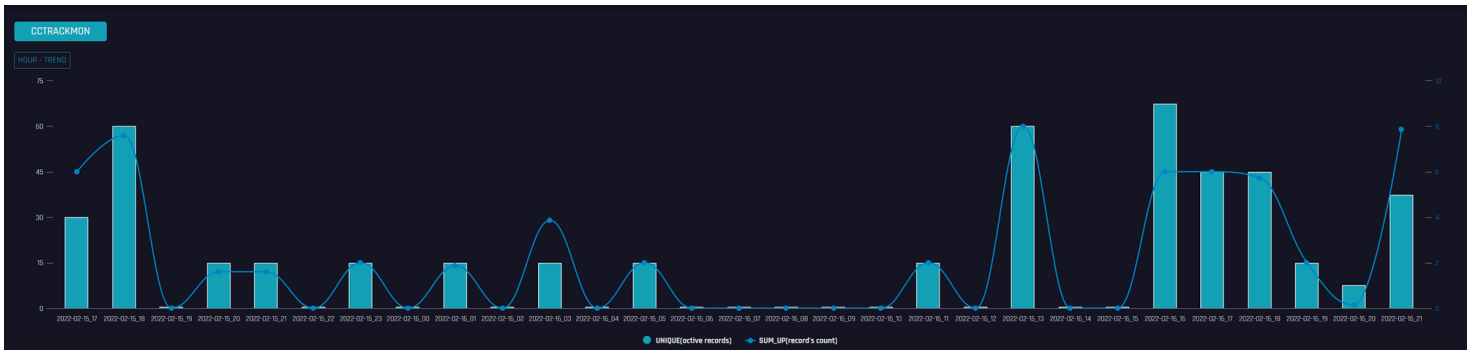
DDoS attacks against Ukraine

The chart below shows the trend of attacks we have seen against **some** of the government websites.



You can see that the attacks started as early as February 12, and continued to grow in number and intensity, peaking on February 16, with a mix of NTP amplification, UDP/STD/OVH floods, and other types of attacks.

Below is the DDoS attack we saw against another website ending in `.ua`, “online.oschadbank.ua”.



This particular C2 came online on 2/11 and sent its first attack command to its bots at 2022-02-16 03:02:37+08:00, and it only launched attacks targeting four 185.34.x.x/24 IPs(all belongs to UA bank oschadbank.ua), the last attack commands we received from it is at 2022-02-17 01:08:27+08:00. We informed security community internally about this C2 and consequently it has be taken down.

Other than the NTP amplification attacks, the majority of DDoS attacks captured are botnet based, so far involving five different types of botnets(mirai, gafgyt,

ircbot,ripprbot,moobot), more than 10 unique C2 IPs. Here we are not going to go over all the C2s' technique details, but some brief breakdowns on 4.

1, mirai_5.182.211.5

As mentioned earlier, this C2 attacked only one target, "oschadbank.ua", during its active period (2022-02-11 to 2022-02-17). Our honeypot saw its samples continuously, and some of the URLs and MD5s are:

```
e5822f8f9bc541e696f5520b9ad0e627        http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv
39532b27e2dbd9af85f2da7ff4519467        http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv
69b51b792b1fca9a268ce7cc1e1857df        http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv
70aaa4746150eba8439308096b17d8cc        http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv
68ed4532bd6ad79f263715036dee6021        http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv
54bd85b40041ba82ae1b57664ee3e958        http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv
1b7247a2049da033a94375054829335d        http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv
ac4d8d0010775e185e12604c0e304685        http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv
0eca53a2dca6384b7b1b7de186e835b5        http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv
cc79916e1e472a657a9ae216b2602a7b        http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv
8f488f3218baec8b75dc6e42e5c90a47        http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv
b307dd0043e94400f8632c4d0c4eae0e        http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv
340255b25edf28c8de140f3f00306773        http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv
e2b103a3b74dd0bfd98ffd27ed07f2c6        http://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv
```

The samples are all Mirai variant with strong Mirai code features, retaining typical Mirai functions such as table_init() and attack_init(). The following are some of the attack commands it sent to its bots.

```
2022-02-16 21:27:44+08:00       mirai           5.182.211.5                     6019
2022-02-16 21:19:04+08:00       mirai           5.182.211.5                     6019
2022-02-16 21:06:14+08:00       mirai           5.182.211.5                     6019
2022-02-16 19:17:12+08:00       mirai           5.182.211.5                     6019
2022-02-16 18:55:07+08:00       mirai           5.182.211.5                     6019
2022-02-16 18:34:18+08:00       mirai           5.182.211.5                     6019
2022-02-16 18:15:23+08:00       mirai           5.182.211.5                     6019
2022-02-16 17:55:35+08:00       mirai           5.182.211.5                     6019
2022-02-16 17:39:01+08:00       mirai           5.182.211.5                     6019
2022-02-16 17:24:37+08:00       mirai           5.182.211.5                     6019
2022-02-16 17:24:37+08:00       mirai           5.182.211.5                     6019
2022-02-16 16:48:55+08:00       mirai           5.182.211.5                     6019
2022-02-16 13:41:41+08:00       mirai           5.182.211.5                     6019
2022-02-16 13:25:49+08:00       mirai           5.182.211.5                     6019
2022-02-16 13:23:33+08:00       mirai           5.182.211.5                     6019
2022-02-16 11:06:32+08:00       mirai           5.182.211.5                     6019
2022-02-16 05:04:45+08:00       mirai           5.182.211.5                     6019
```

```
2022-02-16 01:02:32+08:00       mirai           5.182.211.5                 6019
2022-02-15 23:00:06+08:00       mirai           5.182.211.5                 6019
2022-02-15 21:00:08+08:00       mirai           5.182.211.5                 6019
2022-02-15 20:01:13+08:00       mirai           5.182.211.5                 6019
2022-02-15 18:55:36+08:00       mirai           5.182.211.5                 6019
2022-02-15 18:30:32+08:00       mirai           5.182.211.5                 6019
2022-02-15 18:08:50+08:00       mirai           5.182.211.5                 6019
2022-02-15 17:42:26+08:00       mirai           5.182.211.5                 6019
```

2, mirai_209.141.33.208

The sample of this C2 has been available since January 25, and the timeline of it dropping samples is shown in the figure below.

It launched attack against “www.szru.gov.ua” on the 16th.

```
2022-02-16 05:35:38+08:00       mirai           209.141.33.208              209.1
```

3, gafgyt_172.245.6.134

The sample of this C2 started to spread as early as January 29, and the corresponding timeline of sample dropped is.

The following are some of the attack commands we received.

```
2022-02-17 01:46:30+08:00       gafgyt          172.245.6.134               6110
2022-02-17 00:08:31+08:00       gafgyt          172.245.6.134               6110
2022-02-17 00:07:40+08:00       gafgyt          172.245.6.134               6110
2022-02-16 22:19:04+08:00       gafgyt          172.245.6.134               6110
2022-02-16 22:18:33+08:00       gafgyt          172.245.6.134               6110
2022-02-16 22:07:34+08:00       gafgyt          172.245.6.134               6110
2022-02-16 22:01:44+08:00       gafgyt          172.245.6.134               6110
2022-02-16 21:57:02+08:00       gafgyt          172.245.6.134               6110
2022-02-16 21:53:16+08:00       gafgyt          172.245.6.134               6110
2022-02-16 21:46:41+08:00       gafgyt          172.245.6.134               6110
2022-02-16 21:44:41+08:00       gafgyt          172.245.6.134               6110
2022-02-16 05:35:27+08:00       gafgyt          172.245.6.134               6110
```

4, gafgyt_188.127.237.5

This C2 sample was captured on February 6, and it attacked the “od.tax.gov.ua” website on February 16.

```
2022-02-16 01:54:00+08:00   gafgyt          188.127.237.5                606     S
```

DDoS attacks against Russia

Below are **some** of the attack we see against Russian websites. Note here only a small number of victims are displayed, as there are just way too many targets the diagram won’t be readable if we show all of them.

We are counting 25 C2s now related to .ru DDoS attacks so far, as mentioned above the raw data is vast we might need to wait for another time to go through more details but here is a list of the C2s.

```
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
ripprbot_171.22.109.201
ripprbot_212.192.246.183
ripprbot_212.192.246.186
```

IoC

```
# C2 mirai_5.182.211.5
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.arc   54bd85b40041
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.arm   5096be3bab6b
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.arm   70aaa4746150
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.arm5  9636a88f8543
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.arm5  cc79916e1e47
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.arm6  8f488f3218ba
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.arm6  c5350546e6d2
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.arm7  59b9988a7132
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.arm7  b307dd0043e9
# hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.i486        49b9
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.i486  e5822f8f9bc5
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.i686  1b7247a2049d
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.i686  c2135973f6d0
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.m68k  456773819380
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.m68k  68ed4532bd6a
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.mips  69b51b792b1f
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.mips  d38cc4879fe0
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.mpsl  39532b27e2db
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.mpsl  69717fbd6954
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.ppc
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.sh4   0eca53a2dca6
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.sh4   b21e118e9f6b
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.spc   340255b25edf
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.spc   84c7c39e3f1a
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.x86   bfaffefb3cc7
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.x86   e2b103a3b74d
hxxp://5.182.211.5/z0l1mxjm4mdl4jjfjf7sb2vdmv/KKveTTgaAAsecNNaaaa.x86_64        8be8


# 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        13ead0d75d2fcdf53c7d6d8f40f615f4
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     619517a7ff244de1dc574d2ffb6553d3
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

C2 used to attack .ru sites:
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
ripprbot_171.22.109.201
ripprbot_212.192.246.183
ripprbot_212.192.246.186
```

Contact us

Readers are always welcomed to reach us on Twitter or email us to netlab at 360 dot cn.

到第4个版本

Fodcha Is Coming Back, Raising A Wave of Ransom DDoS

卷土重来的DDoS狂魔：Fodcha僵尸网络再次露出獠牙

See all 56 posts →

1. 概述 * 17个云上重点资产有漏洞攻击行为，包括某民主党派市级委员会、某县级中医院等云上重点单位。 * 随着俄乌冲突全面升级，我们发现有攻击者利用Docker Remote API未授权访问漏洞，对俄罗斯境内服务器发起拒绝服务(DoS)网络攻击。 * Apache APISIX本月爆出远程代码执行漏洞(CVE-2022-24112)，攻击者通过两种攻击方式可远程执行恶意代...

Mar 11, 2022 · 9 min read

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...

Feb 25, 2022 · 12 min read