Botnet

CatDDoS系团伙近期活动激增分析

daji, Wang Hao, Acey9, Alex.Turing

2024年5月22日 • 10 min read

概述

XLab `大网威胁感知系统` 会对当前活跃的主流DDoS僵尸网络家族进行持续跟踪和监控，最近3个月，这套系统观察到CatDDoS系团伙持续活跃，利用的漏洞数量达80+，攻击目标数量最大峰值300+/d，鉴于其活跃程度，我们整理了一份近期的各种数据分享给社区以供参考。

漏洞利用

根据视野内的数据，我们观察到CatDDoS系团伙最近3个月使用了大量的已知漏洞传播样本，总数达80多个。具体漏洞如下：

这些漏洞影响的厂商设备如下：

VENDOR NAME	PRODUCT NAME
A-MTK	Camera
Apache	ActiveMQ
Apache	Log4j
Apache	Rocketmq
Avtech	Camera
Barni	Master Ip Camera01 Firmware
Billion	5200W-T Firmware
Cacti	Cacti

VENDOR NAME	PRODUCT NAME
Cambiumnetworks	Cnpilot R190V Firmware
Cisco	Linksys Firmware
Ctekproducts	Skyrouter
DASAN Networks	Dasan GPON home routers
D-Link	DCS-3411 Firmware
D-Link	DCS-930L Firmware
D-Link	DIR-600
D-Link	D-Link DIR-645
D-Link	D-Link DIR-655 Firmware
DrayTek	Vigor2960 Firmware
Eir	D1000 Modem Firmware
Fastweb	Fastgate 0.00.81
FreePBX	FreePBX 13, 14 and 15
Gargoyle	Router
GitLab	GitLab
Gocloud	Router
Gocloud	S2A Wl Firmware
Google	Android ADB
Hadoop	YARN API
Huawei	Hg532 Firmware
Jenkins	Jenkins
LB-LINK	LB-LINK BL-AC1900
LG	LG SuperSign CMS
LILIN	DVR
Linknet-Usa	Lw-N605R Firmware
Linksys	Linksys X3000
Linksys	RE7000
Linksys	Router

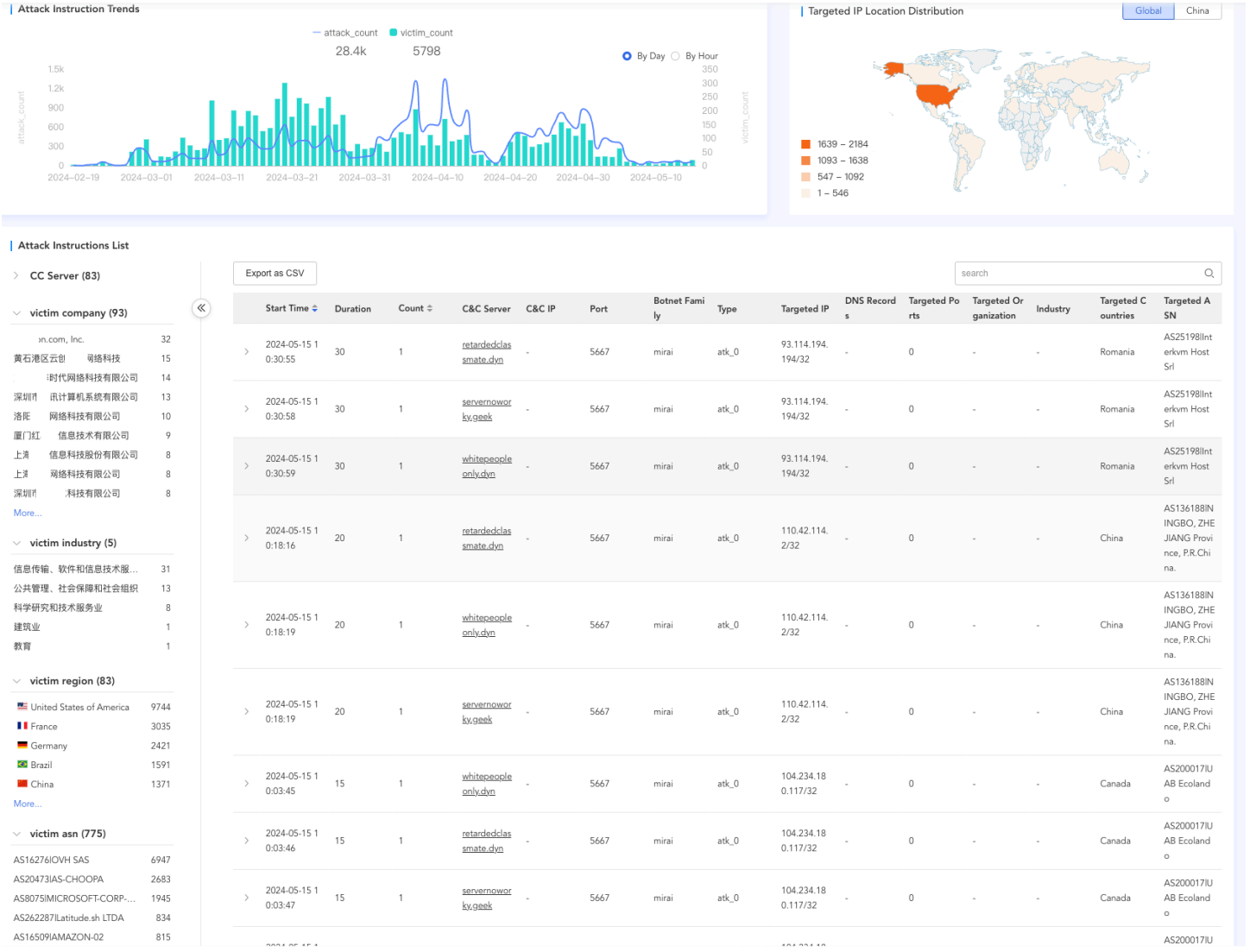
VENDOR NAME	PRODUCT NAME
Metabase	Metabase
Multiple Vendors	CCTV-DVR
MVPower	CCTV DVR
Netgear	DGN1000 1.1.00.48
Netgear	Dgn2200 Series Firmware
Netgear	Netgear R6250
Netis	Router
Nortekcontrol	Linear Emerge Essential Firmware
OptiLink	Router
Realtek	Realtek Jungle SDK
Realtek	SDK
Ruckus	Ruckus Wireless Admin
Seagate	Blackarmor Nas 220 Firmware
Shenzhen TVT	DVR
SonicWall	Global Management System
Tenda	Ac7 Firmware
Tenda	Tenda AC18
Tenda	Tenda AX3
Tenda	W6
Tenda	W9
ThinkPHP	ThinkPHP 5.x
TOTOLINK	A3002R Firmware
TOTOLINK	A3002Ru Firmware
TPLink	Router
TP-Link	TP-Link Archer AX21
UNIMO	DVR UDR-JA1004/JA1008/JA101
University of Texas Health Science Center	Uniview ISC 2500-S
Vacron	NVR

VENDOR NAME	PRODUCT NAME
WIFISKY	L& Router
Yachtcontrol	Yachtcontrol
Zeroshell	Zeroshell
ZTE	F460
ZTE	ZXV10 H108L Router
Zyxel	ATP series firmware
Zyxel	Multiple Zyxel devices
Zyxel	Nas326 Firmware
Shenzhen Hongdian	Hongdian H8922
Ruijie	RG-BCR860
Ruijie	RG-EW1200G

这些漏洞中有些暂时没找到线索来确定是何种漏洞，但根据投递样本的运行参数猜测，可能是0day。比如下图样本运行参数中的skylab0day，Cacti-n0day等。其中我们可以确认`skylab`为黑产人员网络ID。`skylab0day`也许代表着`skylab`提供的0day 漏洞。

DDoS攻击

下图是视野内的数据，从我们的系统中可以方便地查询CatDDoS的历史活跃情况以及各个维度的详细信息比如cc、指令、被打目标等。可以看到CatDDoS攻击目标遍布全球，主要分布在美国、法国、德国、巴西、中国等，被攻击目标分布在云厂商，教育、科研、信息传输、公共管理、建筑等行业。



举个例子，以被攻击的这家名为“上海x网络科技有限公司”为例，可以看到CatDDoS团伙在2024年4月7日晚上9点多对其发动了多次 DDoS攻击，DDoS类型是我们内部命名的atk_0，每次攻击时长为60秒。

这张图则反映了阿联酋电信管理局也曾遭受过类似的攻击。

CatDDoS的衍生

CatDDoS是Mirai的一个变种，因为早期域名和样本里使用了较多"cat"、"meow"而得名，可见其作者是一个十足的猫猫友好人士。视野中CatDDoS最早出现在2023年8月份，这份早期报告与我们发现的时间相近，且近期样本在通信方面与老版本相比没有太大变化，因此可以作为样本分析部分的参考，本文不再赘述。

通过对Telegram相关频道的观察，我们推测CatDDoS应该就是去年12月份关停的Aterna Botnet，该频道的历史消息如今已经删除，下图是作者在群里发布的关停通知。在关停后由于出售或泄露了源代码，导致陆续出现了新的变种，比如RebirthLTD、Komaru、Cecilio Network等。

以下是当时我们在Telegram相关群中发现的泄露文件，这名用户曾在群里多次询问是否有人要购买，可能长时间的无人问津或者购买者数量较少，导致其直接放出了源代码，不幸的是相关历史纪录可能已被删除，还好我们当时及时保存了文件。通过比较样本以及源代码，我们发现和CatDDoS基本一致。

虽然不同变种可能由不同团伙运营，但在代码、通信设计、字符串、解密方法等方面变化不大，因此我们统一将这些变种归为CatDDoS系，尽管他们可能不愿意承认，然后我们简单梳理了一下不同变种出现的时间线（忽略vapebot）。

CatDDoS系变种较多，我们列出几个曾经较为活跃的变种及其特点，如下图所示。

近期比较活跃的两个变种是 `v-2.0.4 (CatDDoS)` 和 `v-Rebirth (RebirthLTD)`，在通信时都使用了chacha20作为数据加密方法，key和nonce也一模一样，不同点在于v-2.0.4使用了opennic域名作为C2。`RebirthLTD` 在历史上也曾用过原始的mirai代码进行开发，后改为使用CatDDoS源码且更新频繁。v-snow_slide未曾公开披露，曾经活跃过一段时间，现在已经沉寂，下文会单独介绍。v-ihateyou仅仅是我们的一个猜测，从C2特征的角度关联为CatDDoS系，但通信机制和字符串解密方面不太符合CatDDoS的特点，而是沿用了Mirai的设计，并且这个变种只是昙花一现。

整体来看，CatDDoS系的样本没有太多变化，只是相较于老旧版本来说，从不加壳->加壳、带符号->去掉了符号，以此来增加逆向的难度。所以结论是：有变化但变化不大。

未曾披露的v-snow_slide

v-snow_slide最早发现于2023年10月，在Aterna关停后 v-snow_slide的指令数量骤降，我们推测v-snow_slide还是由Aterna开发运营。通过逆向分析发现保留了大量Fodcha僵尸网络的代码，比如运行成功后输出"snow slide"、使用xxtea解密字符串、使用OpenNIC域名作为C2、在通信协议部分也拥有相同的switch-case结构以及流量加密算法（xxtea+chacha20），莫非是Fodcha借尸还魂？此外比较有意思的是这个变种在上线时使用了诸如`N3tL4b360G4y`、`paloaltoisgaytoo`等字样，表达了作者对于安全厂商的“致敬”。

模板共用

这里是我们观察到的一个比较有意思的情况：模板共用问题。所谓的模板共用就是不同团伙之间使用了相同的源代码进行二次开发，简单修改后就投递上线，当然这在IoT僵尸网络方面屡见不鲜，比如相似的字符串配置、C2通信设计、加解密方法等，因此botnet的同源性研究也是一个比较有意思的点。而本次我们发现，至少还有三个家族用了和CatDDoS相同的chacha20算法，并且是完全相同的key/nonce，可以自行验证一下😂。

```
key = b'\x16\x1e\x19\x1b\x11\x1f\x00\x1d\x04\x1c\x0e\x08\x0b\x1a\x12\x07\x05\x09\x0
nonce = b'\x1e\x00\x4a\x00\x00\x00\x00\x00\x00\x00\x00\x00'
init_counter = 1
catddos: b6f06dea3dc7597067958cfcdc81f00dfd868a32
hailbot: 65c754d58c150067641689a73e7e124fa936e17b
woodman: 2d732a2f45394691437ff3fcfca2198a63e32b17
vapebot: 61ac7c3f4ea855e68aa11f1f988531ed25c83859
```

本是同根生，相煎何太急

在分析被打目标的时候，除了前文所说的“正常的目标”之外，我们发现很多被打目标是其他变种或其他家族的C2设施，和我们长期在Telegram频道中观察到的情况大概一致，不同运营者之间的摩擦冲突不断，这或许是IoT僵尸网络的另一特色，不仅限于CatDDoS。

```
2024-04-06 07:24:26 rebirth-network.su -> 185.234.66.97(omgnoway.geek)
2024-04-12 08:46:50 omgnoway.geek -> 45.142.182.80(cnc.tsuki.army)
2024-04-12 09:07:47 omgnoway.geek -> 87.246.7.66(rebirth-network.su)
2024-04-12 17:18:41 rebirth-network.su -> 185.234.66.97(omgnoway.geek)
2024-04-17 04:02:45 9wg0dstmud.pirate -> 87.246.7.66(rebirth-network.su)
2024-04-17 13:05:35 secure-core-rebirthltd.su -> 45.142.182.80(cnc.tsuki.army)
2024-04-26 23:41:51 45.142.182.80(cnc.tsuki.army) -> retardedclassmate.dyn
2024-04-27 17:37:19 retardedclassmate.dyn -> 212.70.149.13(RebirthTLD Download Serv
```

对此我们只想说：

总结

本文分享了我们当前掌握的关于CatDDoS的近期情报，以及如何使用我们的大网威胁感知系统来进行威胁分析，对我们的研究感兴趣的读者可通过 Twitter 联系获取更多详细信息。

IoC

Sample

```
5a1124cee1a26f84aa151a68e1dbdebd6fe7a247
f34e17c84d66117156826997aec6136e10d7cb9e
c8fdd11675b5e2df18815eb098d2568f5cf9a232
b6f06dea3dc7597067958cfcdc81f00dfd868a32
5538eb7e09395f5bfefae1af26b4c17cb5631da0
7f55aab44fd9939c7a0c81d78838d81991209ec4
b9f7237d0058c069d500891811356d9f2c6f0692
d9d569b0567dd406bf09c33e4ac71966138fbbd2
4681e012013921c539d155861338adc4630d8f38
e81dc79de33af42ee6e9e489ae1305165649ef28
4e7c2c86b37d7f44ef2f80974cc60c068e205526
3665a8652b068332615ddd1d2e9a19b63f0d2475
```

Domain

```
catddos.pirate
i-like-dicks.pirate
chinks-eat-dogs.africa
jm1hj56glo.pirate
siegheil.hiter.su
omgnoway.geek
phhfr59rqd.parody
9wg0dstmud.pirate
hsjupldf2z.pirate
9fz0cqekwr.parody
4m8mdkx76o.indy
fd9vsneghh.libre
chinkseatblahajs.libre
francothesped.geek
akira-cuddles-blahajs.pirate
rebirthltd.dev
scan.rebirthltd.dev
rebirthltd.com
scan.rebirthltd.top
xysk5eeyj0j5n.xyz
lsagjogu8ztaueghasdjsdigh.cc
fuck-niggers.xyz
secure-core-rebirthltd.su
```

```
secure-network-rebirthltd.ru
hitler.su
kz.hitler.su
bot.secure-network-rebirthltd.ru
security.secure-core-rebirthltd.su
vps.rebirth-network.su
kz.adolfhitler.su
security.rebirth-network.su
sex.secure-cyber-security-rebirthltd.su
rebirth-network.su
cecilioisbetter.dyn
iswearshewas18.geek
thisisnotabotnet.pirate
whitepeopleonly.dyn
servernoworky.geek
retardedclassmate.dyn
cecilio.network
cecilio.pro
shrug.lol
cumshot.vip
tlscat.net
chink.site
chink.online
zerlhocantcompete.dyn
3djd83hf4.geek
2x26ucbyaq.parody
```

IP

```
212.70.149.10   Bulgaria|None|None      AS204428|SS-Net
212.70.149.14   Bulgaria|None|None      AS204428|SS-Net
87.246.7.194    Bulgaria|Sofia|Sofia    AS204428|SS-Net
87.246.7.198    Bulgaria|Sofia|Sofia    AS204428|SS-Net
87.246.7.66     Bulgaria|Sofia|Sofia    AS204428|SS-Net
89.32.41.31     Romania|Timis|Timisoara AS48874|HOSTMAZE INC SRL-D
103.161.35.44   The Netherlands|Noord-Holland|Amsterdam AS0|
31.220.1.44     The Netherlands|Noord-Holland|Amsterdam AS206264|Amarutu Technology
194.169.175.20  The Netherlands|Noord-Holland|Amsterdam AS211760|Suisse Limited
194.169.175.31  The Netherlands|Noord-Holland|Amsterdam AS211760|Suisse Limited
194.169.175.39  The Netherlands|Noord-Holland|Amsterdam AS211760|Suisse Limited
194.169.175.40  The Netherlands|Noord-Holland|Amsterdam AS211760|Suisse Limited
194.169.175.43  The Netherlands|Noord-Holland|Amsterdam AS211760|Suisse Limited
```

What do you think?

3 Responses

 Upvote

 Funny

 Love

 Surprised

 Angry

 Sad

1 Comment Login ▾

G

Join the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

♡ Share

Best Newest Oldest