Botnet

CatDDoS-Related Gangs Have Seen a Recent Surge in Activity

daji, Wang Hao, Acey9, Alex.Turing

2024年5月22日 • 8 min read

- Overview
- Exploited Vulnerabilities
- Targets of DDoS
- Derivation
- Undisclosed v-snow slide
- Template Sharing
- Cannibalism
- Conclusion
- IoC
  - Sample

Domain

IP

Overview

XLab's CTIA(Cyber Threat Insight Analysis) System continuously tracks and monitors the active mainstream DDoS botnets. Recently, our system has observed that CatDDoS-related gangs remain active and have exploited over 80 vulnerabilities over the last three months. Additionally, the maximum number of targets has been observed to exceed 300+ per day. So we decided to share some recent data with the community for reference.

Exploited Vulnerabilities

According to the data in our field of view, we have observed that CatDDoS-related gangs' samples have used a large number of known vulnerabilities to deliver samples in the past three months up to 80+. The specific vulnerabilities are as follows.

These vulnerabilities affect the following vendor devices.

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

VENDOR NAME	PRODUCT NAME
Cacti	Cacti
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

VENDOR NAME	PRODUCT NAME
Linksys	Router
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

VENDOR NAME	PRODUCT NAME
Vacron	NVR
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

We have not yet identified some vulnerabilities, but it may be a 0-day vulnerability based on the parameters of execution of the samples. For example, "skylab0day" and "Cacti-n0day" are shown in the sample's running parameters in the figure below. We can confirm that "skylab" is the network ID of black production personnel among them. "skylab0day" may represent a 0-day vulnerability provided by "skylab".

Targets of DDoS

The following figure displays the data of DDoS. Our system allows easy access to the historical activity of CatDDoS-related gangs and detailed information about various dimensions such as cc, instruction, target, etc. We can notice that CatDDoS-related gangs' targets are distributed worldwide, with the main focus in the United States, France, Germany, Brazil, and China. These targets are distributed across cloud vendors, education, scientific research, information transmission, public administration, construction, and other industries.

Let's take the company "Shanghai * Network Technology Co., LTD." as an example, the CatDDoS-related gangs initiated numerous DDoS attacks on the company after 9 p.m. on April 7, 2024 and the DDoS type is atk_0 which is an internal designation and each attack lasted 60 seconds.

This figure illustrates a similar attack on the UAE Telecommunications Authority.

Derivation

CatDDoS is a variant of Mirai from the beginning, which is named because of the use of "cat" and "meow" in early domain names and samples, showing that its author is a completely cat-friendly guy. CatDDoS first appeared in August 2023. This early report is close to the time we found. In addition, the recent sample has

not changed much compared with the old version in terms of communication, so the report can be used as a reference for sample analysis.

Along with observing Telegram channels related to the topic, we hypothesized that CatDDoS might have been shut down in December last year. The Aterna botnet's channel message history has been deleted. Below is a shutdown notification posted by the author in the group. Due to the sale or leak of the source code, new variants emerged, such as RebirthLTD, Komaru, Cecilio Network, etc. after the shutdown.

The following image shows the leaked file that we found in a Telegram group. At that time, the user had repeatedly asked if anyone wanted to buy in the group. Maybe nobody asked for it for a long time or the number of buyers is small, leading to the direct release of the source code. Unfortunately, the relevant history may have been deleted, but we saved the file in time. By comparing the samples and the source code, we found that it is basically the same as CatDDoS.

Although the different variants may be managed by different groups, there is little variation in the code, communication design, strings, decryption methods, etc., so we unified these variants into the CatDDoS-related gangs, even though they may not want to admit it, and then we briefly ran through the timeline of the emergence of the different variants (just ignore the vapebot).

There are many variants of CatDDoS-related gangs' sample, we list several variants that were once more active along with their characteristics, as shown in the figure below.

Two variants that have been active recently are ***v-2.0.4 (CatDDoS)*** and ***v-Rebirth (RebirthLTD)***, both of which use chacha20 as a data encryption method for communication, and key and nonce are identical. The difference is that v-2.0.4 uses the OpenNIC domain name as C2. RebirthLTD was also historically developed using the original code of Mirai, but switched to the code of CatDDoS later and updated frequently. v-snow_slide, which has not been publicly disclosed, was active for a while but is now silent, as described separately below. The variant named v-ihateyou is just a guess from the perspective of cc characteristics associated with the CatDDoS and the communication mechanism and string decryption do not conform to the characteristics of CatDDoS, but follows the design of Mirai and this variant is just a flash in the wind.

Overall, the CatDDoS-related samples have not changed much compared with the old version. It changes from "no shell" to "modified upx shell" and "with symbols" to "remove symbols" just in order to increase the difficulty of reverse analysis. So the conclusion is that there is change but not too much.

Undisclosed v-snow_slide

The version named v-snow_slide was first discovered in October 2023, and the number of v-snow_slide commands plummeted after Aterna shut down and we assume that v-snow_slide was developed and operated by Aterna. Analysis of reverse engineering found that a large number of Fodcha codes were retained. For example, output "snow slide", use xxtea encryption, use OpenNIC domain name as C2, and have the same switch-case structure and traffic encryption algorithm (xxtea+chacha20) in the communication protocol. Could it be Fodcha coming back from the dead? In addition, it is more interesting that this variant uses words such as ***'N3tL4b360G4y'*** and ***'paloaltoisgaytoo'*** while checking in online with C2 which expresses the author's "tribute" to the security company.

Template Sharing

We also noticed something else interesting: "Template Sharing". This refers to different groups using the same source code for malware development. Attackers just make simple modifications and deliver them online then. This practice is common in IoT botnets, where similar string configurations, C2 communication designs, and encryption/decryption methods are used so Researching the homology of botnets is also an interesting point. We've found that at least three other families use the same chacha20 algorithm as CatDDoS, along with the exact same key/nonce. You can verify this yourself 😂.

```
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
```

Cannibalism

When analyzing the targets of DDoS, we found that many of the targets were other variants or other families' C2 facilities in addition to the "normal target" mentioned above, which matches the situation we observed in the Telegram channel, friction between different operators constantly conflict, which may be another feature of the IoT botnet. Not limited to 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
```

What can we say?

Conclusion

This article shares the recent data we have on CatDDoS-related gangs and how to use our CTIA(Cyber Threat Insight Analysis) System for threat analysis. Readers interested in our research can contact us on Twitter for more details.

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?

7 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

L

lll fff

9 months ago