HNS Botnet

HNS (Hide and Seek), a new range of Bonet is widely infecting IoT devices. The sample was captured by our honeypot system and has control over thousands of IoT devices all around the world which includes,

- AVTECH IP Camera
- TP Link Routers
- Cisco Linksys Routers
- Netgear Routers

Also includes Open Source NoSQL Databases such as,

- OrientDB
- CouchDB

HNS IoT botnet is second of the kind which uses P2P communication after Hajime. The P2P node addresses are hard-coded with the binary.

The malware identifies the victims conducting a port scan over “80”, “8080”, “23” and many other open random ports. Also scans for OrientDB and CouchDB ports such as “2480” and “5984”.

The malware on infection does the following activities:

1. Self Deletion
2. Modification of IPTable rules by adding a rule

```
-A INPUT -p udp -m udp --dport 27651 -j ACCEPT
```

3. File Additions
    + /sys/module/xt_tcpudp
    + /sys/module/xt_tcpudp/srcversion
    + /sys/module/xt_tcpudp/notes
    + /sys/module/xt_tcpudp/notes/.note.gnu.build-id
    + /sys/module/xt_tcpudp/taint
    + /sys/module/xt_tcpudp/initstate
    + /sys/module/xt_tcpudp/coresize
    + /sys/module/xt_tcpudp/sections
    + /sys/module/xt_tcpudp/sections/.init.text
    + /sys/module/xt_tcpudp/sections/.text
    + /sys/module/xt_tcpudp/sections/__mcount_loc
    + /sys/module/xt_tcpudp/sections/.rodata
    + /sys/module/xt_tcpudp/sections/__verbose
    + /sys/module/xt_tcpudp/sections/.strtab
    + /sys/module/xt_tcpudp/sections/.symtab
    + /sys/module/xt_tcpudp/sections/.gnu.linkonce.this_module
    + /sys/module/xt_tcpudp/sections/.rodata.str1.1

+ /sys/module/xt_tcpudp/sections/.rodata.str1.8
+ /sys/module/xt_tcpudp/sections/.note.gnu.build-id
+ /sys/module/xt_tcpudp/sections/.exit.text
+ /sys/module/xt_tcpudp/sections/.data..read_mostly
+ /sys/module/xt_tcpudp/refcnt
+ /sys/module/xt_tcpudp/uevent
+ /sys/module/xt_tcpudp/holders
+ /sys/module/xt_tcpudp/initsize
+ /sys/module/x_tables/holders/xt_tcpudp
+ /dev/pts/1

The binary is a UPX packed binary and after unpacking we get the hardcoded P2P IP list and port numbers as in the screenshot is shown below:

```
  :    0x0805cf24           das
 ,===< 0x0805cf25           jp   0x805cf81
 |:    0x0805cf27           xchg eax, esi
 |:    0x0805cf28           retf
 |:    0x0805cf29           inc  esp
 |:    0x0805cf2a           mov  edi, 0xd10d7a7d
 |:    0x0805cf30           int3
 |:    0x0805cf31           mov  al, 0xda                    ; 218
.----> 0x0805cf33           insb byte es:[edi], dx
:|:    0x0805cf34       ~   sbb  byte [esi + 0x36], bh
:|:    ;-- "~64*s":
:|:    0x0805cf35          .string "~64*s" ; len=6
 |:    0x0805cf3b           or   eax, 0xa21ff51e
 |:    0x0805cf40           nop
,====< 0x0805cf41           jg   0x805cf7e
||:,=< 0x0805cf43           jmp  0xbcc07167
||:|   0x0805cf48           cmp  ebp, ecx
||:,=< 0x0805cf4a           je   0x805cfbb
|||||  0x0805cf4c           xor  edx, esp
|||||  0x0805cf4e           pop  edx
|||||  0x0805cf4f           add  al, 0xde
|||||  0x0805cf51       ~   fidiv word [ebx]
|||||  ;-- "3S&4":
|||||  0x0805cf52          .string "3S&4" ; len=5
|||||  0x0805cf57           mov  dword [0xbf3e545a], eax     ; [0xbf3e545a:4]=-1
|||||  0x0805cf5c           stosd dword es:[edi], eax
|||||  ;-- "'t4iy":
|||||  0x0805cf5e          .string "'t4iy" ; len=6
|||||  0x0805cf64           outsd dx, dword [esi]
|||||  0x0805cf65           fiadd dword [0xd2bb2fcb]
|||||  0x0805cf6b           enter 0x59b7, 0x13
|||||  0x0805cf70           mov  ah, 0xdb                    ; 219
|||||  0x0805cf72           shl  edi, 1
 ||`==< 0x0805cf74           jns  0x805cf0a
||  ||  0x0805cf76           retf 0xfffffffffffb285
||  ||  0x0805cf79           or   ebx, edi
||  ||  0x0805cf7b           scasd eax, dword es:[edi]
```

Fig: 1.1

Operation:

A random UDP check packet is sent (Fig: 1.2). Then starts a socket SYN connection to each IP in the list and communicates to the one which answer on the specified ports (23,80,8080) (Fig: 1.3).

No.	Time	Source	Destination	Protocol	Lengtl	Info
1	0.000000	10.0.2.15	79.68.193.115	UDP	49	27651 → 16208 Len=7
2	0.000188	10.0.2.15	212.212.217.95	TCP	54	33933 → 7595 [SYN] Seq=0 Win=65446 Len=0
3	0.000243	10.0.2.15	18.77.206.33	TCP	54	33933 → 7595 [SYN] Seq=0 Win=65446 Len=0

```
⊞ Frame 1: 49 bytes on wire (392 bits), 49 bytes captured (392 bits)
⊞ Ethernet II, Src: PcsCompu_4c:9f:46 (08:00:27:4c:9f:46), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
⊞ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 79.68.193.115
⊟ User Datagram Protocol, Src Port: 27651, Dst Port: 16208
    Source Port: 27651
    Destination Port: 16208
    Length: 15
    Checksum: 0x1ce7 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
⊟ Data (7 bytes)
    Data: 9dfd865b1413c7
    [Length: 7]
```

Fig: 1.2

329	2.071882	10.0.2.15	223.151.63.54	TCP	54	33933 → 80 [SYN] Seq=0 Win=65446 Len=0
330	2.071905	10.0.2.15	187.254.223.72	TCP	54	33933 → 80 [SYN] Seq=0 Win=65446 Len=0
331	2.071929	10.0.2.15	159.195.116.166	TCP	54	33933 → 80 [SYN] Seq=0 Win=65446 Len=0
332	2.071948	10.0.2.15	93.127.51.232	TCP	54	33933 → 80 [SYN] Seq=0 Win=65446 Len=0
333	2.071971	10.0.2.15	10.0.2.2	TCP	54	33933 → 80 [SYN] Seq=0 Win=65446 Len=0
334	2.071997	10.0.2.15	10.0.2.3	TCP	54	33933 → 80 [SYN] Seq=0 Win=65446 Len=0
335	2.094219	10.0.2.3	10.0.2.15	TCP	60	80 → 33933 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
336	2.094259	10.0.2.2	10.0.2.15	TCP	60	80 → 33933 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
337	2.121185	202.76.226.103	10.0.2.15	TCP	60	80 → 33933 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
338	2.255777	46.16.247.248	10.0.2.15	TCP	60	80 → 33933 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
339	2.255810	94.176.174.176	10.0.2.15	TCP	60	80 → 33933 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=
340	2.255828	10.0.2.15	94.176.174.176	TCP	54	33933 → 80 [RST] Seq=1 Win=0 Len=0
341	2.289157	125.227.181.175	10.0.2.15	TCP	60	80 → 33933 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
342	2.319093	121.98.196.133	10.0.2.15	TCP	60	80 → 33933 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
343	2.330648	190.106.203.133	10.0.2.15	TCP	60	80 → 33933 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
344	2.470070	211.55.238.62	10.0.2.15	TCP	60	80 → 33933 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
345	3.401986	10.0.2.2	10.0.2.15	ICMP	70	Destination unreachable (Host unreachable)
346	3.516459	10.0.2.2	10.0.2.15	ICMP	70	Destination unreachable (Host unreachable)
347	3.537040	177.29.152.95	10.0.2.15	TCP	60	80 → 33933 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
348	3.931512	10.0.2.15	81.124.201.190	UDP	49	27651 → 18687 Len=7
349	3.931672	10.0.2.15	94.176.174.176	TCP	74	34642 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
350	3.931719	10.0.2.15	255.75.123.193	TCP	54	33933 → 23 [SYN] Seq=0 Win=65446 Len=0
351	3.931746	10.0.2.15	27.159.202.42	TCP	54	33933 → 23 [SYN] Seq=0 Win=65446 Len=0
352	3.931776	10.0.2.15	97.233.43.41	TCP	54	33933 → 23 [SYN] Seq=0 Win=65446 Len=0
353	3.931804	10.0.2.15	233.169.179.4	TCP	54	33933 → 23 [SYN] Seq=0 Win=65446 Len=0
354	3.931847	10.0.2.15	58.219.161.235	TCP	54	33933 → 23 [SYN] Seq=0 Win=65446 Len=0

Fig: 1.3

An IP “78.134.51.161” connected on P2P network with HNS providing IP camera feed on an HTML page (Fig: 1.5).

```
8055 110.729094    78.134.51.161    10.0.2.15        HTTP    647 HTTP/1.1 200 OK  (text/html)
8056 110.729135    10.0.2.15        78.134.51.161    TCP      54 54771 → 80 [ACK] Seq=40 Ack=594 Win=30243 Len=0
8057 110.729231    10.0.2.15        78.134.51.161    TCP      54 54771 → 80 [RST, ACK] Seq=40 Ack=594 Win=30243 Len=0

    File Data: 341 bytes
Line-based text data: text/html
    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">\n
    <html>\n
    <head>\n
    \n
    </head>\n
    <body>\n
    <p><a href="http://camaiana.myq-see.com/zm/index.php?view=watch&mid=3&scale=50" name="IP CAM">\n
      <img src="camera.png"/>\n
    </a>\n
    <a href="http://camaiana.myq-see.com/zm" name="Control Center">\n
      <img src="postazione.png"/>\n
    </a>\n
    \n
    </p>\n
    </body>\n
    </html>\n
    \n
```

Fig: 1.4

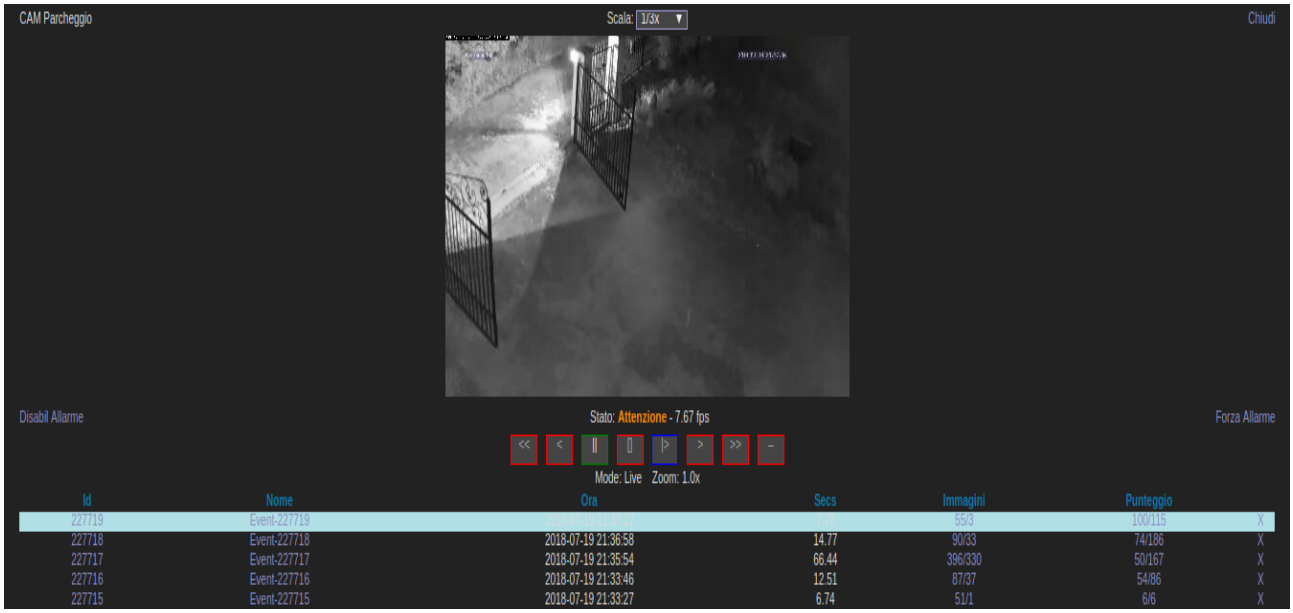

Fig: 1.5

The HNS IoT Botnet does nto have any entries for maintaining persistance and so a simple reboot will clean the infection from the devices.

Exploits used for the HNS infection can be found here:

https://www.exploit-db.com/exploits/40500/
https://www.exploit-db.com/exploits/42965/
https://www.exploit-db.com/exploits/44913/

SubexSecure Protection:

SubexSecure detects the samples of HNS botnet as **“SS-HNS-ELF.Gen.A”**

IOCs:

Sample Hashes

```
96f6fe32e918024cfcf86ae5015a06bc
2852596c6dbb91cc3a2ab5203f12dda1
70e07244823e92b7c77513b68c5e3487
e6096f4319a8da74855978162c740f28
bf07642dfe8348770996c7709835cfe8
d18db976adb956d5a16c0cb227263488
14b788d4c5556fe98bd767cd10ac53ca
1a710ce00757f25ffbf2dca340d5f3c7
020be51161114673202e044a3e41fcc4
68d52da9a7dc9b79a5f4687b13662752
9a038c039225bf9287a8fc61ccf6b087
44bb76c2785ac25bd7bea9b5607abf59
ec79e69c86eaf0c342c9572044cb37a9
01a92f88b1ac97555a91c7358657e95d
87e4902b74654defe5081263bb4a750d
3df0479fdc85f07b1de8c0818d569297
67d7e71c8d5ec2af9889abfc96f4472f
f5984362959cde659d5419388557c35c
ff4b90230aa11427ebd0e58edcbd30bb
9dedcd1a95fd858ed7ea33284e7cf286
1d6450f0563a2fd87eccce06c141df75
d19e0a1454e3fb861a842d96ff5c64fb
a2decc3b87b4e4d6e3e2738292acde05
```

Connecting IP's:

```
31.162.144.127:15337
31.162.155.226:40671
31.162.186.180:15337
31.163.101.192:15305
58.212.173.111:34354
58.218.160.221:26164
58.52.16.130:10758
58.57.77.44:58552
59.0.118.224:62769
59.0.234.239:34097
81.198.6.174:26575
81.214.137.97:40985
85.154.11.246:56214
85.248.27.178:62797
86.217.213.64:17636
89.138.129.172:22888
89.19.180.219:53735
91.245.159.189:6075
92.27.196.33:46941
94.240.31.7:62797
94.50.200.120:40671
94.50.227.57:15305
94.50.238.221:15305
94.51.159.182:15337
101.83.218.153:54389
108.35.3.149:12721
109.13.47.51:12809
```

109.223.191.136:155
109.223.94.201:4617
110.137.154.41:17760
113.240.46.8:14766
113.28.59.233:1037
115.186.91.173:62797
115.53.203.207:13876
116.111.51.212:23044
117.81.180.140:54941
121.132.101.118:64981
121.148.202.133:45579
121.163.127.5:54727
121.189.111.218:1483
122.136.44.149:30260
122.238.82.203:5120
122.254.32.209:44898
125.86.59.95:1140
149.156.155.29:28729
151.72.10.3:40990
157.25.190.101:19683
162.216.208.43:62797
171.106.226.156:2106
171.124.219.179:46913
178.47.112.85:15337
178.47.177.241:15305
178.47.4.37:15337
179.176.247.35:53721
182.123.163.198:12442
182.126.73.193:12154
182.55.174.8:7986
188.18.255.110:1408
188.19.62.190:1410
189.102.171.157:53697
190.158.241.77:53879
190.204.109.175:34614
190.38.253.207:23014
203.212.96.66:23511
203.98.154.41:45653
211.20.10.88:62107
211.226.1.104:15684
213.59.174.191:63922
218.108.24.126:13876
218.16.184.216:22068
218.186.89.235:36817
221.145.253.66:51102
221.213.123.252:12154
221.238.182.53:5684
222.102.106.107:45023
222.114.198.37:9142
222.164.44.231:53291
31.163.164.147:16063
31.163.43.211:16063
31.163.90.84:16063
31.41.49.125:53735
31.42.29.220:62797
36.24.130.207:52400
37.142.254.96:54795
37.211.51.54:27475
110.4.16.238:54891
112.164.13.57:47112

112.168.183.99:36194
112.171.245.17:5890
112.81.175.108:22068
113.109.217.202:48937
113.193.238.202:5076
113.206.122.117:38450
175.194.48.55:24480
175.201.64.105:27972
177.91.158.178:30295
178.46.19.61:20159
178.46.32.245:15337
178.46.67.111:2945
178.46.91.192:1282
59.15.172.191:15284
59.51.215.177:12442
61.153.146.62:38764
61.244.150.234:57864
69.112.164.75:64251
74.129.51.146:45059
77.91.196.131:53735
78.243.69.10:12809
79.162.238.207:47689
80.13.214.30:28520
183.128.155.252:48953
183.132.198.26:39320
183.216.90.203:58929
185.105.215.207:42270
185.81.80.134:62797
186.188.110.19:8677
187.154.227.164:40985
188.153.27.65:55013
188.17.7.1:40671
1.82.30.204:22089
5.141.87.236:15337
5.43.83.36:62797
5.50.142.106:521
14.189.20.238:31810
14.244.200.198:24464
24.92.153.165:18964
27.20.138.205:12154
94.98.208.160:7869
95.218.25.237:57432
95.226.175.59:5225
97.88.87.202:4583
101.171.39.116:13417
101.81.38.223:4649
37.79.109.216:15305
37.79.46.206:1024
37.79.52.132:11967
42.112.63.115:48451
42.115.248.13:7925
46.77.69.9:52225
47.187.210.243:51383
49.91.240.96:48329
50.247.130.186:26219
118.118.188.44:22716
118.163.245.218:10330
118.40.82.191:50566
118.45.44.182:51067
119.192.113.67:58472

119.207.33.4:43606
121.12.164.244:22068
122.3.49.179:51781
123.151.200.141:26164
123.26.187.209:34497
124.230.0.22:30260
125.122.13.209:52400
125.136.176.122:2969
125.40.10.202:35179
190.75.147.130:22341
193.250.99.166:4617
202.103.51.204:5683
202.109.178.150:9780
203.198.255.111:10455
218.94.114.214:59579
220.246.62.23:8713
221.10.120.233:13876
221.13.9.27:13876
222.222.51.83:9780
222.240.143.141:30260
222.67.223.84:45849
223.175.70.158:52585
90.150.203.68:16063
90.150.243.118:15305

Conclusion:

The HNS botnet is suspected to include functionalities for CPU crypto mining and DDos and information theft.