
29th ANNUAL
FIRST
CONFERENCE
SAN JUAN
PUERTO RICO
JUNE 11-16, 2017
FIGHTING PIRATES AND PRIVATEERS
WWW.FIRST.ORG

Mirai – How Did We Do?

Merike Kaeo – Farsight Security (Moderator)

Martin McKeay – Akamai

Chris Baker – Dyn

Yiming Gong – Qihoo 360

Megat Muazzam Abdul Mutalib - MyCERT

Early Warnings

Martin McKeay

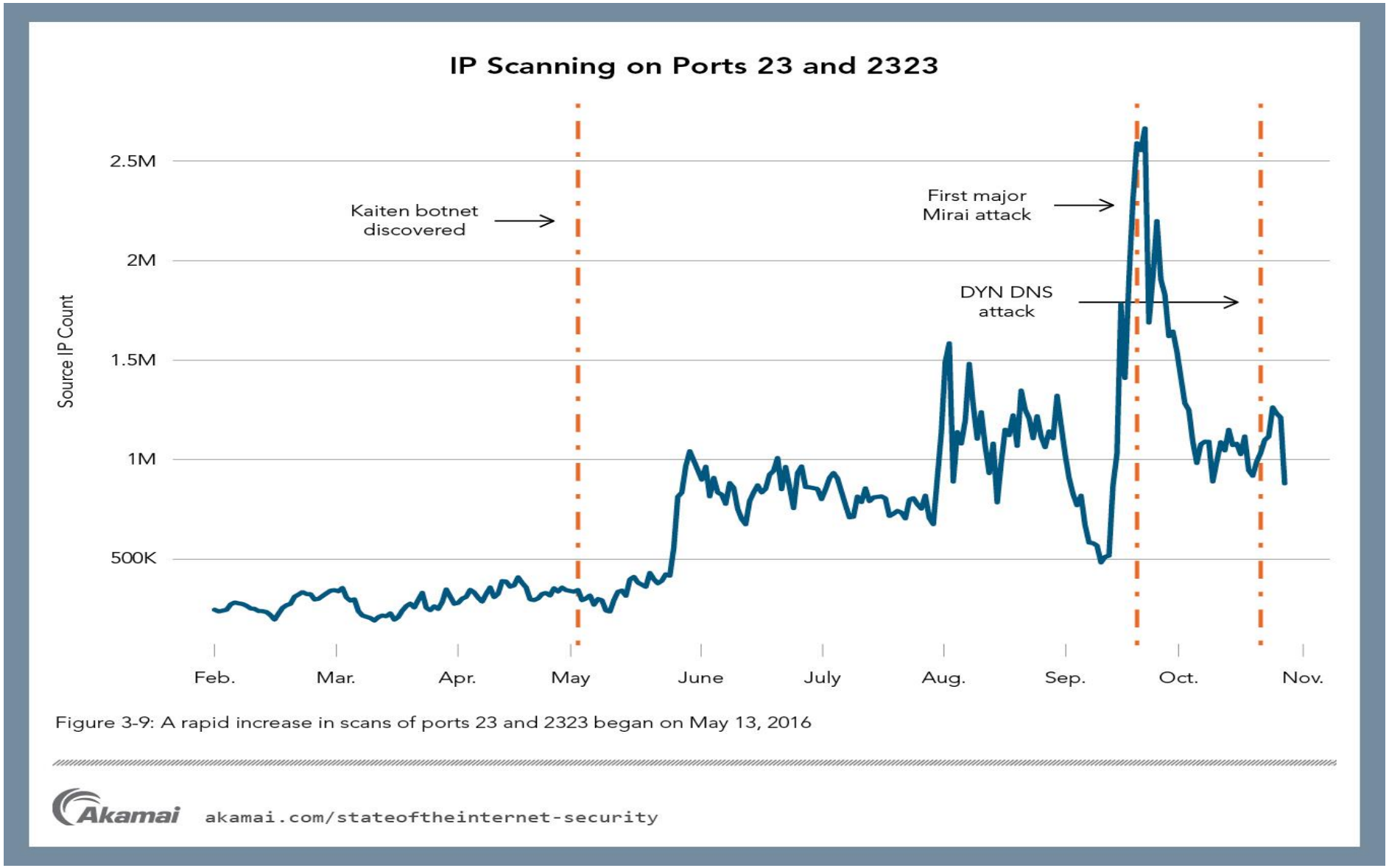


Figure 3-9: A rapid increase in scans of ports 23 and 2323 began on May 13, 2016

Akamai akamai.com/stateoftheinternet-security

DNS Signals

Chris Baker

29th ANNUAL FIRST CONFERENCE
SAN JUAN PUERTO RICO

Signals: Patterns In the DNS

- August 2016 in-protocol (properly formed DNS packets) DDos attacks
- A large volume of properly formed protocol queries
  - Pseudo-random sub domains prepended to cause a cache miss
    - Example: lq18v2V3N2lQ.<sub domain>.<domain>.<tld>
    - The 12 character pseudorandom string attached to the valid domain was a consistent attribute Example: Gk4d85kg4qrl.datumrich.com
    - “Random” excluding values ‘xyz’ and ‘9

Fingerprinting: Timing is Everything

- Identify the characteristics of the Mirai SYN vs other SYNs
- For each IP sending Mirai SYN packets use Lift to identify the device
  - https://github.com/trylinux/lift
- IP addresses which are assigned by DHCP (Dynamic Host Configuration Protocol) by ISPs (Internet Service Providers) change for one of four main reasons:
  - A client is disconnected from the network / loses power
  - A client is rebooted or reconnected causing a PPP, point to point protocol over ethernet or ATM, to change address
  - Changes are made by the provider example: restarting the DHCP
  - The provider limits the duration that a lease due to network limitations

https://labs.ripe.net/Members/ramakrishna_padmanabhan/reasons-dynamic-addresses-change

The DNS: Beyond Basic Name Resolution

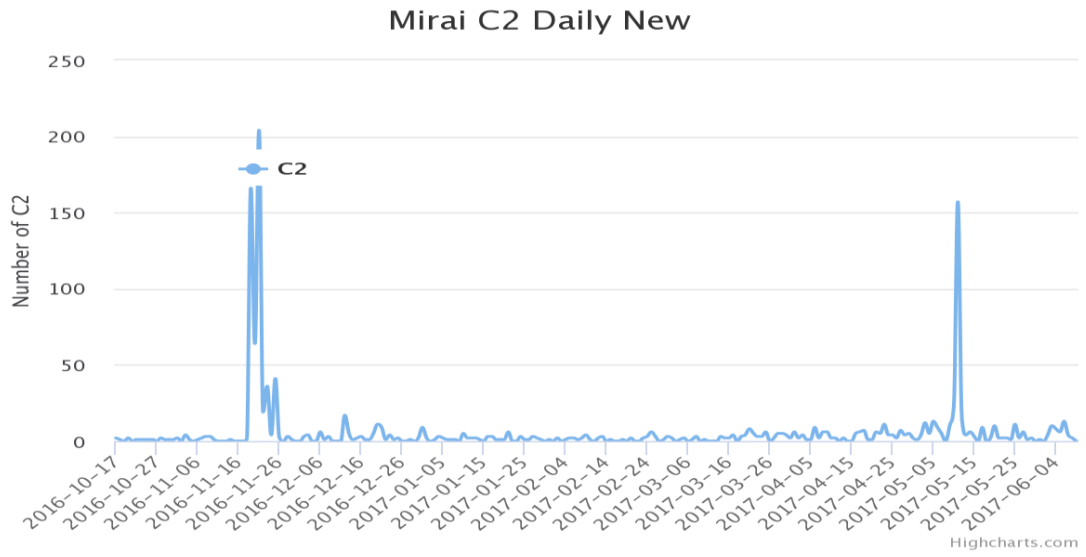
- The DNS is increasingly used to implement traffic management
  - Load balancing / Geo Specific response / CDN management
- The TTL set determines the stickyness of the response
  - Example: If the A / CNAME record fastest-path.example.com has a TTL of 3600, once a resolver asks an authoritative it shouldn't ask again for 3600 seconds (plus or minus X based on pre-fetching and popularity)
  - If attacker
    - When TTL of record is long – Attack endpoint
    - When TTL of record is short – Attack the DNS

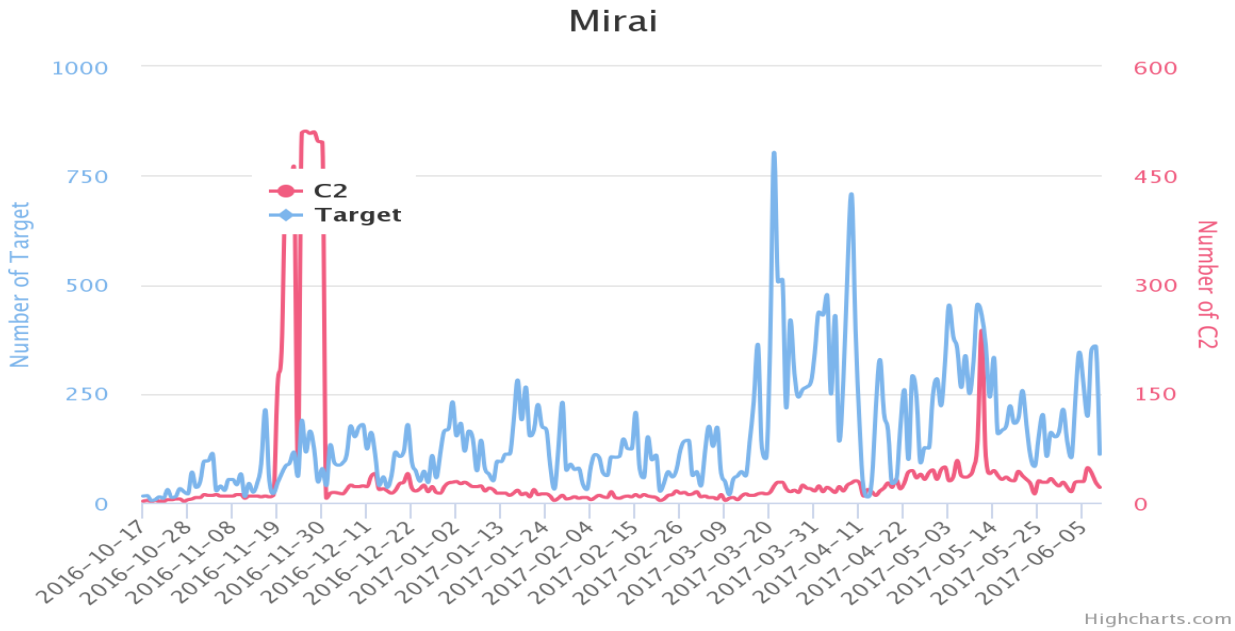
Scanning and Added Correlation

Yiming Gong

Mirai is Something in the Past?

- Daily new C2s, active C2s and Victims





Mirai made its name from Krebs(9/20) and Dyn(10/21) ddos attack, but there were early signs

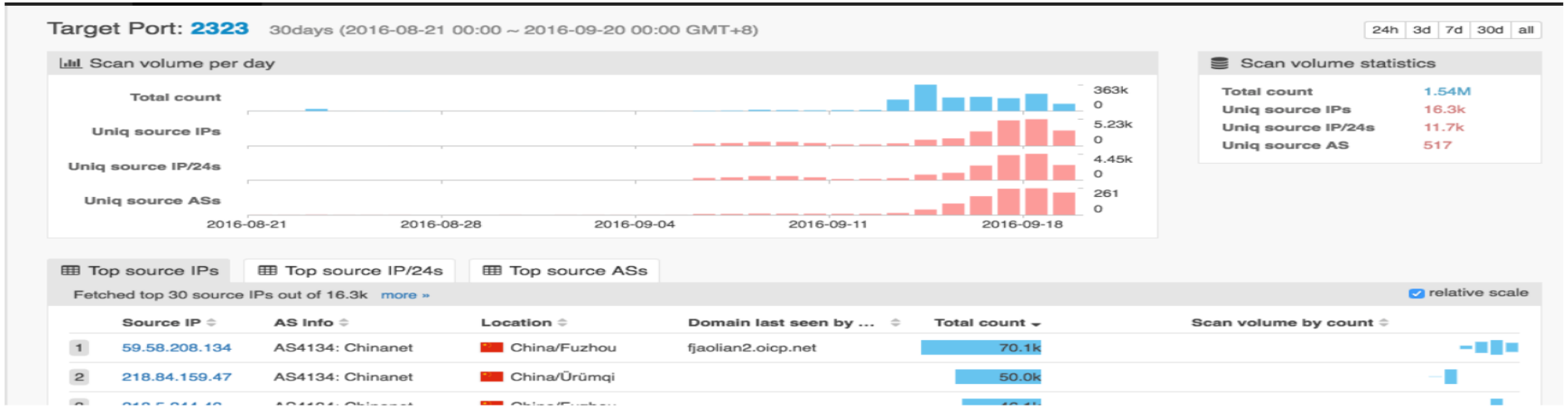
- 9/19 I sent this trust group

Yiming Gong
To: [redacted]
September 19, 2016 at 5:25 AM
YG

port 2323 traffic increase

We have noticed port 2323 scan traffic going up significantly since 6th this month,

http://scan.netlab.360.com/#/dashboard?tsbeg=1471708800000&tsend=1474300800000&dstport=2323&topn=30
(copy|paste the link if outlook replace # with %23)



and our honeypot logs indicate this might have things to do with MIRAI

2016-09-19 17:32:27 INFO: Successful login from 176.35.109.x with credentials admin:123456
2016-09-19 17:32:28 INFO: admin@176.35.109.x entered command: enable
2016-09-19 17:32:29 INFO: admin@176.35.109.x entered command: system
2016-09-19 17:32:31 INFO: admin@176.35.109.x entered command: shell
2016-09-19 17:32:32 INFO: admin@176.35.109.x entered command: sh
2016-09-19 17:32:33 INFO: admin@176.35.109.x entered command: /bin/busybox MIRAI

Mirai made its name from Krebs(9/20) and Dyn(10/21) ddos attack, but there were early signs

- Later I sent this to a trust group

Yiming Gong September 27, 2016 at 3:18 AM

To: [redacted]

Re: correlation with krebsonsecurity ddos attack? was:Re: [redacted] port 2323 traffic increase

Some more observation,

1: a potential c2 for the ddos devices? → **later confirmed is C2: b0ts.xf0.pw**

185.47.62.199 port 5454
we see quite some ddos attack source ips making connection to it, and some of the attack sources are still trying to connect to it right now. (it is not reachable now though)

2: ssh sessions

The following hosts have active telnet sessions with multiple ddos sources between 9/20-9/25
77.247.181.212
77.247.181.213
77.247.181.210
77.247.181.214

3: we also identified some ddos sources are digital harddrive recorder, so they are indeed iot device.

Also News Say Mirai Launched ZYX Gbps Attack

- To us, show me the data or nothing happened
- Better yet, generate the data ourself
  - Nov 01, we found an implementation bug in Mirai
  - Which enabled us to remotely send command to C2s to DDos attack anyone
    - We did a very short test with a Tier 1 ISP (Thanks J!)
    - We saw ~100,000 bots
    - And the attack volume…(really BIG, even crashed some ISP nodes)

Mirai is Also Evolving

- For example, more ports have been added 23,2323,32,19058,22,2222,6789,23231, 37777,7547,5555 and most recently 80,81

- At one point, it enabled DGA, we published our finding on our blog, and registered all the C2 names for the coming month, very shortly, we capture a Mirai sample, which has this encoded.

```
00409070 addiu   $s0, $sp, 0x40+var_28
00409074 jalr    $t9 ; sub_40FA90
00409078 move    $a0, $s0
0040907C lw      $gp, 0x40+var_30($sp)
00409080 move    $a1, $zero
00409084 la      $a0, loc_410000
00409088 la      $t9, sub_414060
0040908C addiu   $a0, (aIloveyouthrees - 0x410000)  # "iloveyouthreesixty"
00409090 jalr    $t9 ; sub_414360
00409094 li      $a2, 0x12
00409098 lw      $gp, 0x40+var_30($sp)
0040909C move    $a0, $s0
004090A0 la      $t9, sub_410010
004090A4 nop
```

And About the C2 Names

- There are some common random generated ones, such as
  - fghdfth.club
  - neuvostoliitto.tk
- There some some look legitimate ones, such as
  - check.securityupdates.us
  - update.kernelorg.download
- But quite some are pretty funny ones, such as
  - heis.lateto.work
  - cannon.lateto.work
  - fuckthefeds.tk
  - malwaremustive.club
  - friend.dancewithme.gq
  - cnc.despairless.cf
  - cloudflarecock.club
  - sheis.lateto.work
  - traplife.ru
  - krebs.fucklevel3.wang
  - immafreebitch.ddns.net
  - imadaddy.us
  - chicken.nigger.press
  - hightechcrime.club

Some Free Statistic and Tools By Us

- Scanmon http://scan.netlab.360.com/
- DDosmon https://ddosmon.net
- mirai-related statistic
  - http://data.netlab.360.com/mirai-c2/
  - http://data.netlab.360.com/mirai-scanner/

Malaysia CERT Perspective

Megat Muazzam Abdul Mutalib

29th ANNUAL FIRST CONFERENCE
SAN JUAN PUERTO RICO

Lessons Learned

- Need to improve the delivery mechanism of the threat intelligent information
- Plan appropriate measure to defend against DDOS attack.
- Improvement in coordination and escalation to respective stakeholder/ISP
- Best Practices to improve/secure IoT devices and applications.

Areas of Improvement

Swift Communication

- Communication is very essential during incidents and for fast mitigations of incidents.

Effective time management

- Management of time among the teams that come from different zones.

Diversity in Analysis Tools

- Having diverse tools and efficient is important for accurate analysis

Right Contacts

- Having right people and right person in charge will ensure incidents are responded fast and efficiently.

Audience Participation

- What was observed in varying regions?
- How effective was information sharing?
- How timely was the information shared?
- What added information would have been useful?
- Is there any change in how Botnet information is shared?