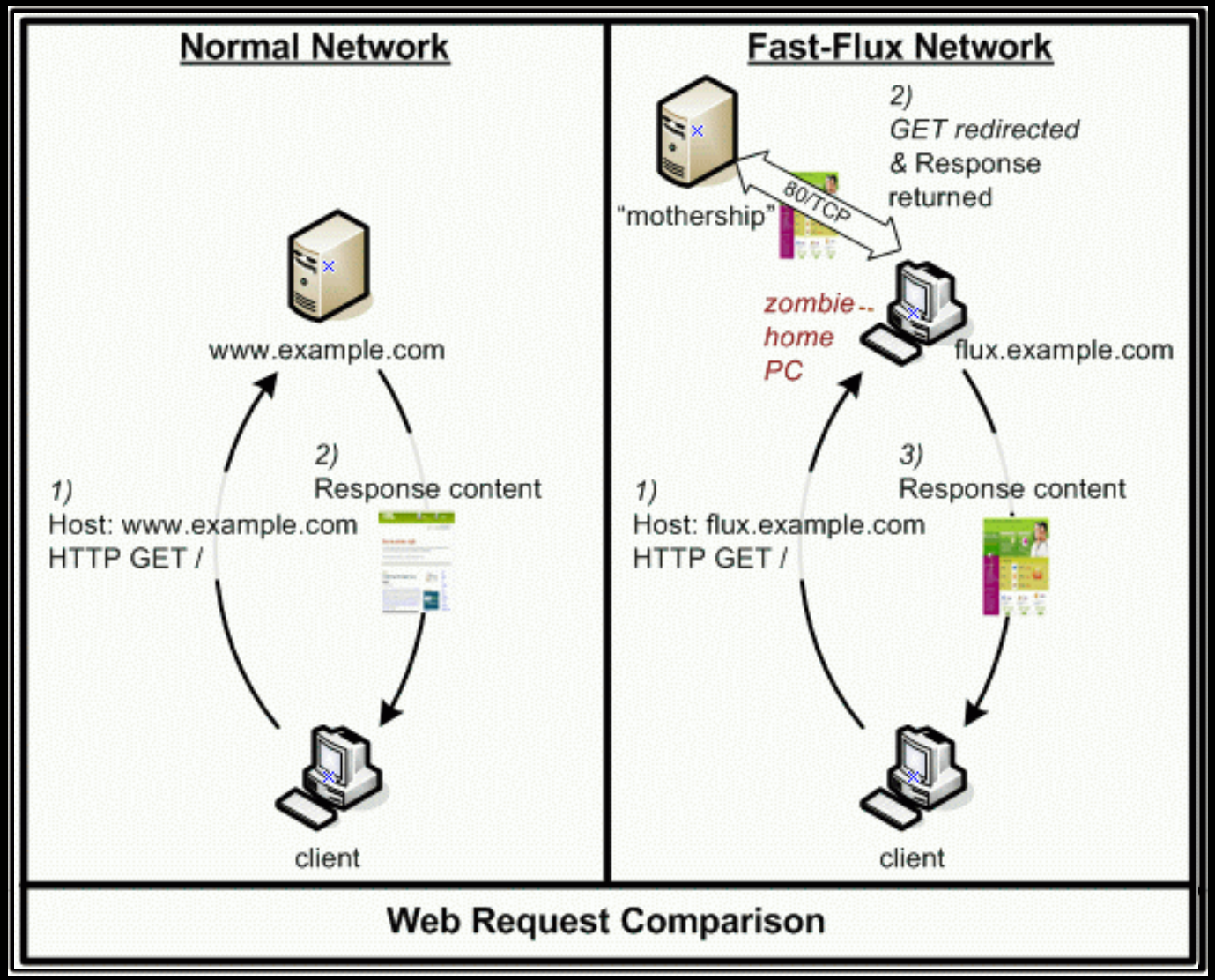
# Think You Know Fast-Flux Domains? Think Again.

New Trends in Fast-Flux Domains

Wei Xu, Xinran Wang
Palo Alto Networks

# What we used to know



# What we used to know

- Malicious content distribution network
- Layer of Proxy
- Rate of change: fast
- Location of change: various

- Attacker's rationale
  - Disposable frontend nodes
  - Long live core backend server (bullet-proof hosting)

# What we know now

- Slower change rate
- Sharing of IP addresses, name servers
- Double-flux OR n-flux
- One IP address at a time
- Clustering

# Slower Change Rate

- "Fast-flux domains' changing rate: < 10 minutes/IP" [1]

- 80% Fast-flux domains > 30 minutes/IP
- Average: 73.55 minutes/IP

| type | Minutes/IP | IP/Day | A-TTL | NS-TTL |
|---|---|---|---|---|
| average | 73.55 | 55.90 | 1832.84 | 37348.75 |
| max | 634.50 | 261.54 | 21598.03 | 65535.00 |
| min | 5.51 | 2.27 | 0 | 0 |

[1] Holz *et.al* ,"Measuring and detecting fast-flux service networks", NDSS'08

# Why Slower?

- It's always about money!
  - Infected hosts are becoming more valuable
    - Valuable assets for bad guys
    - Returned IP can be detected and neutralized
  - Domains are becoming disposable
    - now: $10 per year, 1995: $100 per year
    - short lifetime
- Therefore
  - No need to change so fast
  - Only expose a small part of a botnet
  - Avoid detection (based on changing rate)

# Sharing of IP and Name Servers

- Sharing is everywhere
  - Inter-domains, inter-families, intra-families, etc.
  - Shared IP addresses
  - Shared authority name servers
  - Fast-flux domains do NOT share name servers

| type | number | share-factor (average) |
|---|---|---|
| domain | 207 | n/a |
| name server | 134 | 1.54 |
| authoritative name server | 44 | 4.71 |
| IP | 14440 | 4.52 |

# Why Sharing?

- If an asset is valuable, it is shared
  - Authority name servers are for rent
    - Bullet-proof hosting
  - IP addresses (botnets) are for rent
    - Costs to infect, maintain and operate botnets [2]
- Name servers are no use
  - > 70% name servers share IP with the domain

[2] Max Goncharov ,"Russian Underground 101", Trend Micro TR'12

# How to share?

- Shared IP addresses
  - 1st level:
    - IP addresses are shared among different fast-flux domains using the same authority name server "Control point"
  - 2nd level
    - Among different
    - E.g., 76.27% shar
      "biwcacecca.ru"

| Auth. Name Server | # of domains | % of shared IPs |
|---|---|---|
| atw.kz | 2 | 68.85% |
| biocacces.ru | 5 | 96.15% |
| biwcacecca.ru | 10 | 98.23% |
| blo.kz | 2 | 99.91% |
| xincacec.ru | 10 | 100% |
| xginzecac.ru | 10 | 98.03% |
| sofisale.net | 8 | 80.83% |
| sccacxoec.ru | 9 | 97.81% |
| needhed.com | 15 | 20.32% |
| myhappyplants.com | 8 | 81.33% |
| mkijsppc.ru | 5 | 98.41% |
| kamisca.com | 11 | 6.65% |
| breakwinner.com | 12 | 98.29% |

# Two levels of sharing

- “biocacces.ru” & “biwcacecca.ru”

```
domain:         BIWCACECCA.RU
nserver:        ns1.biwcacecca.ru. 198.144.156.246
nserver:        ns2.biwcacecca.ru. 142.0.79.140
state:          REGISTERED, DELEGATED, VERIFIED
person:         Private Person
registrar:      R01-REG-RIPN
admin-contact:  https://partner.r01.ru/contact_admin.khtml
created:        2013.03.29
paid-till:      2014.03.29
free-date:      2014.04.29
source:         TCI
```

```
domain:         BIOCACCES.RU
nserver:        ns1.biocacces.ru. 198.144.156.246
nserver:        ns2.biocacces.ru. 142.0.79.140
state:          REGISTERED, DELEGATED, VERIFIED
person:         Private Person
registrar:      R01-REG-RIPN
admin-contact:  https://partner.r01.ru/contact_admin.khtml
created:        2013.03.29
paid-till:      2014.03.29
free-date:      2014.04.29
source:         TCI
```

# Inter-malware-family IP sharing

- Trojan: 10% ~ 20% shared IP addresses
  - Trojans serve very different purposes
- Spam: 45% shared IP addresses
  - focus on similar topics
    - E.g., pharmaceuticals, dating, financial, etc.

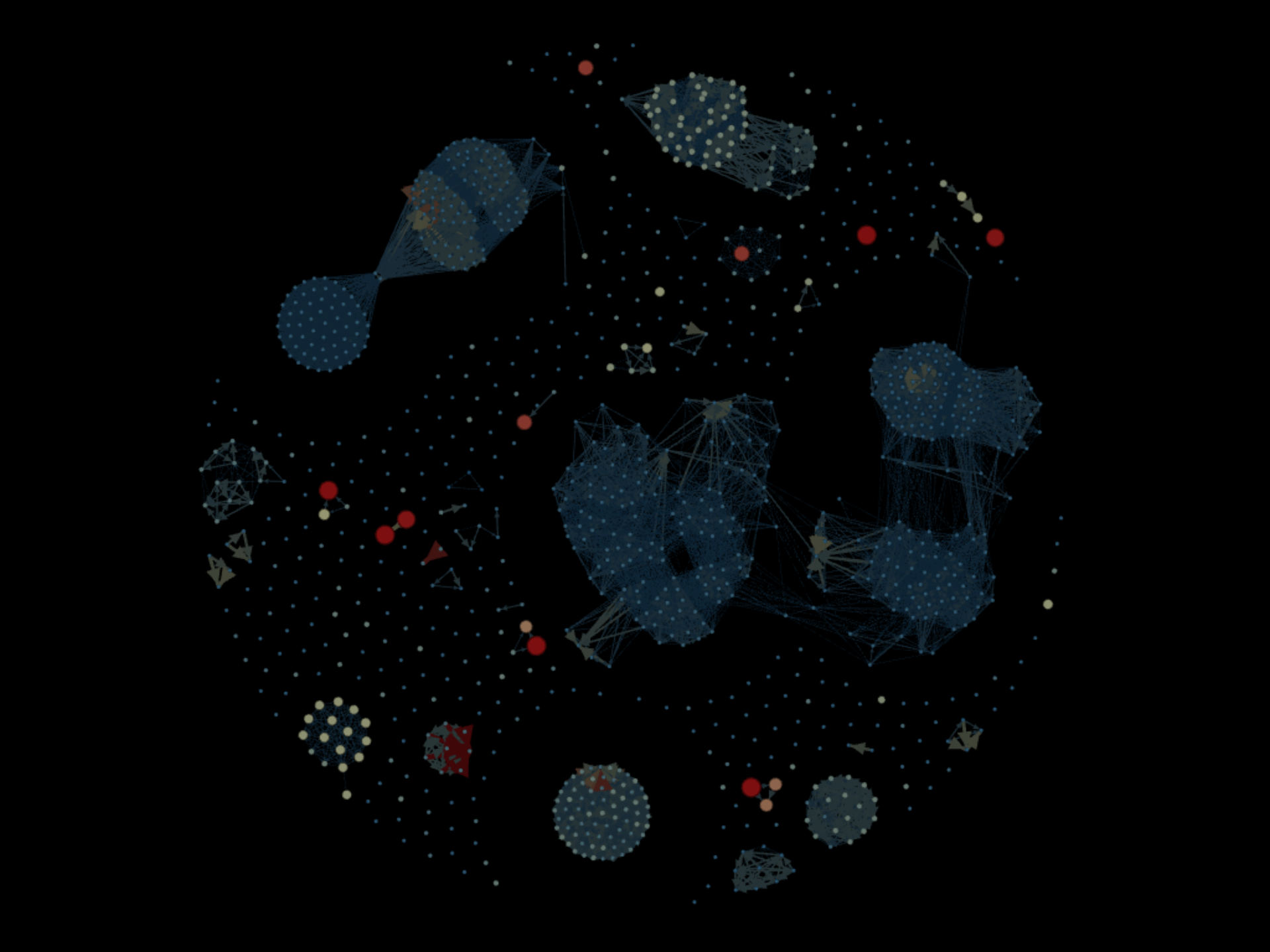
| Type/Family | # of domains | % of shared IPs |
|---|---|---|
| TrojanDownloader.waledac | 8 | 12.36% |
| Trojan.GenericKDZ | 2 | 21.04% |
| Trojan-Psw.tepfer | 2 | 20.30% |
| Trojan-Spy.zbot | 4 | 12.51% |
| spam | 18 | 45.71% |

# N-Flux?

- Double Flux
  - Both A and NS records change
- “N-Flux”
  - The level of NS records appears to be “endless”
    - E.g., “larstor.com” => “ns*. larstor.com” => “ns*.ns*. larstor.com” => and so on
  - Higher levels of name servers are resolved to the same set of IPs as low levels of name servers
  - Wildcard name server, programmed DNS response

# One IP at A Time

- Return one IP address w/ TTL=0
  - Seems like more IPs, right?
- In fact, NO
  - The total number of IP is less than the case where a list of IPs are returned
- Why?
  - Nullify the local DNS cache
  - Give attackers more control
  - Avoid detection



# How the domains are connected

- Content similarity
- Shared IP address
- Shared name server
- Name similarity

# Inter-cluster connections

# What can we learn from cluster?

- Discover the purpose
  - Same cluster serves the similar purpose
- Learn the underground structure
  - E.g., botnet, bullet-proof servers, etc.
- Track family
- Build reputation on entities
  - E.g., IP, name servers
- Find new fast-flux domains

# What looks like Fast-Flux, but NOT

- Distributed Service
  - **NTP pool**
    - use DNS round robin to select NTP server.

      E.g., “pool.ntp.org”
  - **BitCoin DNS seed**
    - use DNS service to discover peer nodes

      E.g., “dnsseed.bluematt.me” => 7747 IP addresses
- Censorship Bypass
    - Leverage DNS to prevent itself from being blocked

      E.g., Dynamic Internet Technology, “*.ziyouforever.com”

# Characteristics of benign “Fast-Flux”

- Faster Change Rate
- HA

| domain | type | Minutes/IP | IP/Day | A-TTL | NS-TTL |
|---|---|---|---|---|---|
| dnsseed.bluematt.me | average | 3.26 | 442.05 | 55.85 | 86400 |
| seed.bitcoin.sipa.be | average | 1.91 | 754.70 | 55.79 | 39148 |
| pool.ntp.org | average | 14.79 | 97.39 | 80.2696 | 3600 |
| download.phoenixai.com.au | average | 17.73 | 81.23 | 59.81 | 65535 |
| *.1.ziyouforever.com | average | 7.32 | 196.66 | 59.98 | 38400 |

- What we can learn from this?
  - “Fast” is no longer the keyword in fast-flux

# How do we collect the data?

- Fast-flux domain candidates
  - Malware samples
  - Public sources
  - Recent domains
- Active monitoring
- Aggregation

# What About Defense?

- Do not rely on changing rate
- Name server reputation score
- Find the connections (via shared IP) among fast-flux domains
- Appeared “N-Flux” structure

# Take Away

- Smarter, smaller, slower Fast-flux networks
- Avoid existing detection approaches

Thank you!
Q & A