Proactively Blacklisting Fast-Flux Networks

Shahan Sudusinghe
shsudusinghe@verisign.com
Verisign iDEFENSE Malcode Operations
What this presentation covers

- Different parts of fast-flux networks
- Different methods to gather fast-flux data
- Why all these different single sources not good enough stand-alone
- How to get a complete picture of an attack
What comprises a fast-flux network

- Domain names
- Authoritative name servers
- IP addresses
- C&C Servers/ Mothership Servers
What are Fast-Flux networks used for:

- Hosting malware
- Launching phishing attacks
- Spam campaigns
- Money Mule scams
- Adult content
Sources to gather FF data

- Trojans that generate them
- Advertising agents (spam, etc...)
- Compromised webservers
- Dropsites, motherships
- Black-list domains/URL Lists from analysis systems

No single source will ever give you the big picture
Why individually these methods not effective?

- IP addresses change all the time
- Attackers retire domains after a while
- Fast-Flux network may not utilize the ONLY source you are monitoring
Collecting FF domains from SPAM

- Collecting SPAM emails through SPAM Traps
- Storm, Weldec, Canadian Pharmacy, Online Pharmacy etc.
- Not limited to e-mails…
Expanding SPAM Traps
SPAM based Fast-Flux monitoring

- [http://dnsbl.abuse.ch](http://dnsbl.abuse.ch) (honeypot based spam collection)
Drop site data & Trojan data

- After infection Trojans report to dropsites
- Infected machines are used in botnets → fast-flux networks
- Identifying Trojan gives more information on the Fast-Flux network
Infected clients used in Fast-Flux hosting

- IP address: 119.95.188.44
  - last seen: 2009-04-27 00:00:00
  - country code: PH
  - parse time: 2009-04-27 00:00:00
  - drop site: Conficker.B Sinkhole == ==

- IP address: 116.68.102.173
  - last seen: 2008-07-08 00:00:00
  - country code: IN
  - parse time: 2008-07-08 00:00:00
  - drop site: Nethell/Limbo == 202.75.38.156 == counter-google sp

- IP address: 121.96.100.139
  - last seen: 2009-04-27 00:00:00
  - country code: PH
  - parse time: 2009-04-27 00:00:00
  - drop site: Conficker.B Sinkhole == ==

- IP address: 121.96.120.157
  - last seen: 2009-05-12 00:00:00
  - country code: PH
  - parse time: 2009-05-12 00:00:00
  - drop site: == 09.208.35.28 == citi-bank.ru

IP address associated with name server

Same IP was reported as infected
Victim IP FF IP aggregation

- With two days worth FF data there was 20 IP matches
- 11 Conficker.B, 4 Zeus, 3 BManager, 1 Limbo and 1 Unknown
- 23 different domains hosting name servers
Rapid Zone Updates (RZU)

- Records every alteration to all authoritative name servers belong to that TLD
- Updates every 5 second interval
- Stores data in flat files
RZU file...

add mayfairadvisors.com NS
add ecasinogoldens.com NS
delete mayfairadvisors.com
add ecasino-goldens.com NS
add ecasino-goldens.com NS
add blueknightspavil.com NS
add ns1.ecasinogoldens.com A 69.57.161.18
add ns1.ecasinogoldens.com A 69.57.161.18
add ilvetrodilivia.com NS
add chondrogenesis.com NS
delete ilvetrodilivia.com
add ecasino-goldens.com NS
add blueknightspavil.com NS
add satng.net NS
add myglobetrip.com NS
add ecasino-goldens.com NS
add satng.net NS
delete satng.net NS ns4.domainsite.com
add ecasino-goldens.com NS
add triptica.net NS
add-new t-1273946207-1240983121197-1-dlqzw.com NS
add satng.net NS
add-new t-1370129124-1240983121258-1-jxnpy.com NS
add triptica.net NS
delete triptica.net NS ns1.domaincontrol.com
delete triptica.net NS ns2.domaincontrol.com
delte t-1273946207-1240983121197-1-dlqzw.com
delete ns2.ecasinogoldens.com A 66.119.68.246
add ns2.ecasinogoldens.com A 66.119.68.246
delte t-1370129124-1240983121258-1-jxnpy.com
add triptica.net NS
add triptica.net NS ns51.domaincontrol.com
add triptica.net NS ns52.domaincontrol.com
delte t-1273946207-1240983121197-1-dlqzw.com
add buysellandconsign.com NS
delete t-1370129124-1240983121258-1-jxnpy.com
add ecasino-goldens.com NS
add mgaffiliatesearnonline.com NS
delete mgaffiliatesearnonline.com NS ns1.renewyourname.net
Double Flux name server

- Use of simple Linux commands to retrieve name servers
- Frequency of change
- Number of IPs associated with it and their net block
- If differs from the reasonably accepted rules it can be flagged as FF (eg name server have 50 IPs)
Reported Fast-Flux on allycom1

<table>
<thead>
<tr>
<th>ID</th>
<th>34762</th>
</tr>
</thead>
<tbody>
<tr>
<td>Url</td>
<td><a href="http://www.buyerguardianinc.com">http://www.buyerguardianinc.com</a></td>
</tr>
<tr>
<td>Domain</td>
<td>buyerguardianinc.com</td>
</tr>
<tr>
<td>ipAddress</td>
<td>89.137.97.175</td>
</tr>
<tr>
<td>Site Name</td>
<td>ѭλβγδεζηθι</td>
</tr>
<tr>
<td>Web Host</td>
<td>δεντγεδδ</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:deng10000@163.com">deng10000@163.com</a></td>
</tr>
<tr>
<td>Status</td>
<td>ok</td>
</tr>
</tbody>
</table>

**Whole**

- Domain Name: BUYERGUARDIANINC.COM
- Registrar: XIN NET TECHNOLOGY CORPORATION
- WHOIS Server: whois.pyscenter.com.cn
- Referral URL: http://www.wenent.com

- Name Server: NS1.ALLYCOM1.COM
- Name Server: NS2.ALLYCOM1.COM
- Name Server: NS3.ALLYCOM1.COM
- Name Server: NS4.ALLYCOM1.COM
- Name Server: NS5.ALLYCOM1.COM

- Status ok
- Updated Date: 10-mar-2009
- Creation Date: 07-mar-2009
- Expiration Date: 07-mar-2010

- Domain Name: buyerguardianinc.com
- Password: buyerguardianinc.com
- Registrant:
  - Organization: xiao rong
  - Name: ding shi
Reported Fast-Flux

The data shows a 19-IP site hosting zombie botnet where the criminal owned nameservers ns1.allycom1.com to ns5.allycom1.com hosted on various rotating IPs are acting as zombie botnet controllers 'herding' the rotating zombies, (as determined by RDNS), in the 'A' records list which are hosting the fraud site (as determined by TRACERT). See The Zombie Botnet 'Host By Proxy' for a general explanation of this method of hosting.

In this instance not only do all of the 'A' record IPs rotate, but also the nameserver hosting, (which is also on either zombies or possibly criminal owned machines), also rotates meaning that ceasing the main and nameserver domain registrations is the only practical method of taking the criminal down. It also means that the above table is simply a snapshot in time - if you plot the main and nameserver host IPs you will get all different ones - there may be hundreds or even thousands of IPs involved.
Domains for Double-Flux

- Difficult to obtain because no changes for name server in RZU
- RZU results has to combined with root zone file data
- Domains always do not belong to one TLD makes it difficult
Single-Flux from RZU + Zone files
Aggregation gives fast results
Aggregation Data Base

- **auth_ns**
  - PK: auth_ns_id
  - FK1: query_id
  - FK: ns_name

- **domain**
  - PK: domain_id
  - FK1: domain_name

- **query**
  - PK: query_id
  - FK1: query_timesource

- **ns_domain_hit**
  - PK: ns_domain_hit_id
  - FK2: domain_id
  - FK1: auth_ns_id

- **domain_ip_hit**
  - PK: domain_ip_hit_id
  - FK1: domain_id

- **ip**
  - PK: ip_id
  - FK2: ip_id
  - FK1: domain_id

- **auth_ns_ip_hit**
  - PK: na_ip_hit_id
  - FK1: auth_ns_id
  - FK2: ip_id
Aggregation Database

- Need to expand to accommodate more data
- Uses series of Python scripts and shell commands to find data
- Uses multiple databases (victimip, spam)
- Currently do not follow domains actively after identification
Don’t wait take action

- Once you find few IP addresses, couple of domains monitor them to find more data
- Black-list/block on the slightest suspicion
- Don’t wait till you know it’s bad
- Data aggregation gives fast results