

**Fast Flux Service Networks**

---

**ANTEL**  
COMUNICACIONES



**CSIIRT**  
GESTION DE INCIDENTES DE SEGURIDAD  
INFORMÁTICA Y DE TELECOMUNICACIONES

**Carlos Martínez-Cagnazzo**  
LACNIC XII  
Panama City  
May 2009

---

---

---

---

---

---

---

---

---

---

**Plan**

- A typical phishing message
- DNS
  - TTL, Round Robin
- Anatomy of a phishing scam
- Fast Flux comes in
- Some conclusions
- References

---

---

---

---

---

---

---

---

---

---

**A typical phishing e-mail**



http://p-216-69-165-83.ip.secureserver.net/cgi-script/temp/login.htm

---

---

---

---

---

---

---

---

---

---

## A typical phishing e-mail (2)

- Para que el *phishing* "funcione" hacen falta:
  - Un sistema comprometido donde alojar las páginas web que simulan al sitio "real"
  - Una forma de direccionar (nombre o IP), para dirigir a los usuarios al mismo
    - En general, las IPs de los sistemas mas frecuentemente comprometidos son variables, por hacen falta nombres para enmascarar esto
  - El **nombre** a usar debería "parecer" genuino
  - Un agente de recolección de datos
    - Drop-boxes o similar




---

---

---

---

---

---

---

---

## DNS (I)

- DNS: Domain Name System
- Basic purpose:
  - Translate IP addresses into textual names more suitable for the human Internet user
- Additional features:
  - Support different services, akin to a directory service
    - Example: e-mail and the MX record
  - Domain sub-delegation
    - Zones, authority
  - Reverse resolution
    - Reverse: mapping IP address to a name

---

---

---

---

---

---

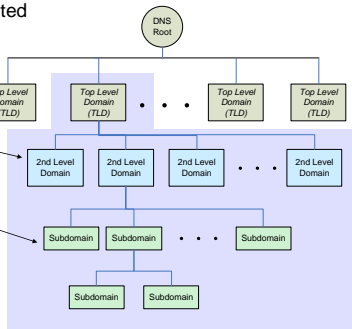
---

---

## DNS (II)

- DNS is a distributed database

- Each sub-domain can be «delegated» and be administered by a different «authority»
- Each «zone» contains records (A, MX, CNAME, etc.)
- Each «zone» points to a delegated zone by using «glue» (NS) records




---

---

---

---

---

---

---

---

### DNS (III)

- Domain name structure:
- To observe:
  - The levels (that is, the dots) are the border between delegations
  - The tree's root is always present but never shown
  - You can have as many levels as you want
  - Upper levels **delegate** authority to the lower ones

---

---

---

---

---

---

---

---

### Round Robin DNS

- Usually employed for:
  - Load balancing
  - Fault tolerance
- Idea:
  - A DNS query can return many records for the same name
  - The DNS server will return these records in different order each time
- Drawbacks:
  - No feedback from the load balances services to DNS
  - Reaction to failers as slow as the record's TTL

|                |      |             |
|----------------|------|-------------|
| www.google.com | IN A | 10.11.20.21 |
| www.google.com | IN A | 1.2.3.4     |
| www.google.com | IN A | 50.55.60.65 |
| www.google.com | IN A | 10.11.20.21 |
| www.google.com | IN A | 1.2.3.4     |
| www.google.com | IN A | 4.5.6.7     |

---

---

---

---

---

---

---

---

### Time-to-Live

- A DNS query is expensive
  - DNS servers can be far away in network terms
  - Queries may involve recursion
- DNS query results are stored in a local resolver cache
- For how long? *Time-to-Live* or record TTL
- Typically
  - 86400 segundos (1 día)
  - Can be as low as 1 second

---

---

---

---

---

---

---

---

## A "problem" for the attackers...

- Blocking / disabling
  - Once detected, a traditional phishing site can be quickly and easily blocked by a service provider. Un sitio de phishing
    - They only need to apply some access list of the WAN port of the customer
  - A botnet's software distribution channel can be easily blocked once a C&C center is detected.
  - Network admins usually take immediate action against these kind of malicious sites
- So the attacker asks himself... *How can I make my botnet network admin and ISP-proof?*

---

---

---

---

---

---

---

---

## And the "answer" is...

- Eliminate all single points of failure
  - Web Server
    - Usually a compromised system somewhere in the world is used to host the phishing pages
  - Name resolution
    - The URL the attacker is sending in his phishing emails must be resolved into an IP address
- *Fast Flux Service Networks* come into the picture
- Modes
  - *Single flux*: Web server only
    - Malicious web server no longer a single system, but a host of them
      - Many "A" records for the phishing URL
  - *Double flux*: Name resolution added to the picture
    - Distributed name resolution
      - Many «NS» records for the phishing URL

---

---

---

---

---

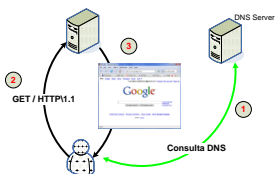
---

---

---

## Anatomy of a FFSN

- Normal web access: [www.google.com](http://www.google.com)



- Different stages
  1. Query DNS looking for "A" record for [www.google.com](http://www.google.com)
  2. Using this result, send HTTP request to web server
  3. Index HTML page is returned

---

---

---

---

---

---

---

---

## Anatomy of a FFSN: Different Types

- *Single Flux*
  - Many web servers for the same site
    - Hosted in many compromised systems controlled by a central entity (a *botnet*)
  - Limited DNS servers
    - Hosted in normal hosting/service providers
      - Admin must allow quite low TTL values in order for the FFSN to be effective
- *Double Flux*
  - Multiple web servers
  - Multiple DNS servers
    - DNS hosting must allow dynamic configuration of NS records with low TTL values

---

---

---

---

---

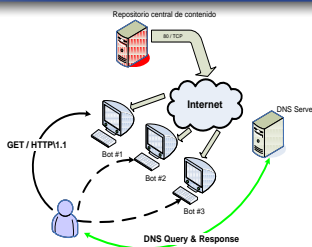
---

---

---

## Anatomy of a FFSN: Single Flux

- How is it different from a "normal" web access?
  - Multiple "A" records (many, 10 – 20 or more can be seen)
  - TTLs muy pequeños
  - "Servers" are compromised office / home PCs
  - «A» records change with time. When a machine is cleaned up, it is taken out from the FFSN
- DNS servers as usual
  - Few records
  - Hosted in a a service provider
- Other comments
  - Web content is fed from a central location by the attacker
    - Easier to manage!




---

---

---

---

---

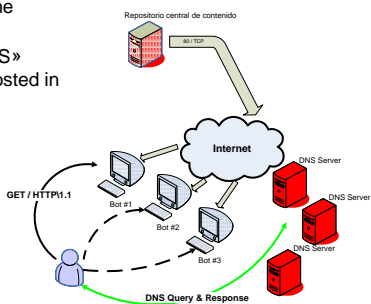
---

---

---

## Anatomy of a FFSN: Double Flux

- *Double flux* adds redundancy to name resolution
- In this case the «NS» records are also hosted in the bots




---

---

---

---

---

---

---

---

## Detecting FFSNs

- Holz et al [1] propose a scoring system in order to detect FFSNs
- Some components of the score:
  - **nA**: number of "A" records returned by a query
  - **nNS**: number of "NS" records returned by a query
  - **nASN**: number of different autonomous systems hosting the "A" records

---

---

---

---

---

---

---

---

## Detecting FFSNs (2)

- Other criteria:
  - IPs reverse names showing that the IPs correspond to an ADSL or dialup service
  - Temporal variations of **nA** and/or **nNS**
    - The botnet continually adapts to bot failures and take downs
  - Low TTLs in the different records
- Software
  - FFDetect
    - Java library, Wellington University, New Zealand, *Open Source*
  - ffdetect.pl
    - Script Perl, CSIRT-Antel, *Open Source*

---

---

---

---

---

---

---

---

## An example of a detected FFSN

- Domain "81dns.ru" (output of dig 81dns.ru)

```
;; ANSWER SECTION:
81dns.ru.      600    IN     A      61.64.210.29
81dns.ru.      600    IN     A      61.224.132.13
81dns.ru.      600    IN     A      68.200.93.27
81dns.ru.      600    IN     A      69.14.27.151
81dns.ru.      600    IN     A      70.196.175.168
81dns.ru.      600    IN     A      71.234.239.212
81dns.ru.      600    IN     A      81.202.211.11
81dns.ru.      600    IN     A      85.90.9.24
81dns.ru.      600    IN     A      85.225.209.183
81dns.ru.      600    IN     A      89.36.58.189
81dns.ru.      600    IN     A      99.149.197.114
81dns.ru.      600    IN     A      124.125.176.244
81dns.ru.      600    IN     A      210.97.124.66
81dns.ru.      600    IN     A      220.129.81.51

;; AUTHORITY SECTION:
81dns.ru.      345586 IN     NS     ns1.81dns.ru.
81dns.ru.      345586 IN     NS     ns2.81dns.ru.
81dns.ru.      345586 IN     NS     ns3.81dns.ru.
```

---

---

---

---

---

---

---

---

## An example of a detected FFSN (2)

- Reverse resolution of "81dns.ru"'s "A" records

```

29.210.64.61 PTR 61-64-210-29-adsl-tpe.dynamic.so-net.net.tw.
13.132.224.61 PTR 61-224-132-13.dynamic.hinet.net.
27.93.200.68 PTR 27-93.200-68.tampabay.res.rr.com.
151.27.14.69 PTR dl4-69-151-27.try.wideopenwest.com.
168.175.196.70 PTR 168.sub-70-196-175.myvzw.com.
212.239.234.71 PTR c-71-234-239-212.hsd1.ct.comcast.net.
11.211.202.81 PTR 81.202.211.11.dyn.user.ono.com.
24.9.90.85 PTR 24.9.90.85.lully.cust.dynamic.gepowernet.ch.
183.209.225.85 PTR c-b7die155.82-6-64736c12.cust.bredbandsbolaget.se.
114.197.149.99 PTR adsl-99-149-197-114.dsl.chcgil.sbcglobal.net.
51.81.129.220 PTR 220-129-81-51.dynamic.hinet.net.

```

---

---

---

---

---

---

---

---

---

---

---

---

## Final Conclusions

- FFSNs can:
  - Provide redundancy and stability for any network used to serve malicious content
  - They provide an additional layer of anonymity to those operating these kind of networks
    - It is next to impossible to obtain logs from a compromised home PC that acts as a botnet webserver
  - ISPs must be careful with the DNS management tools they provide their customers. These tools should include sanity checks like for example limitations on how many changes per hour can the user make
- Good procedures to help in the tracking and take down of these networks are needed

---

---

---

---

---

---

---

---

---

---

---

---

## Referencias

- [1] Holz T., Gorecki C., Rieck K. and Freiling F. C. "Measuring and Detecting Fast-Flux Service Networks": <https://pi1.informatik.uni-mannheim.de/filepool/research/publications/fast-flux-ndss08.pdf>
- [2] Know Your Enemy: Fast Flux Service Networks: <http://www.honeynet.org/papers/ff/fast-flux.html>
- [3] SSAC Advisory 025: SSAC Advisory on Fast Flux Hosting and DNS: <http://www.icann.org/en/committees/security/sac025.pdf>
- [4] Nazario J., Holz T. "As the Net Churns: Fast Flux Service Networks Observations"; MALWARE'08: <http://honeyblog.org/junkyard/paper/fastflux-malware08.pdf>

---

---

---

---

---

---

---

---

---

---

---

---

## Referencias

- [5] ATLAS from Arbor Networks, Fast Flux Summary Report:  
<http://atlas.arbor.net/summary/fastflux>

---

---

---

---

---

---

---

---

*Thanks!*

**ANTEL**

**CSIRT**  
GESTION DE INCIDENTES DE SEGURIDAD  
INFORMÁTICA Y DE TELECOMUNICACIONES

---

---

---

---

---

---

---

---