Fast Flux Service Networks

ANTEL

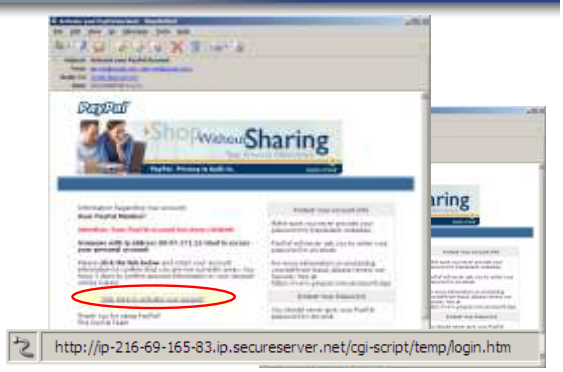
CSIRT

Carlos Martínez-Cagnazzo
LACNIC XII
Ciudad de Panamá
Mayo de 2009

Plan de la Presentación

- Anatomía de un mensaje de *phishing*
- DNS
  - TTL, Round Robin
- Anatomía de un *phishing*
- Fast Flux
- Conclusiones / Referencias

Un mensaje de *phishing* típico



Un mensaje de *phishing* típico

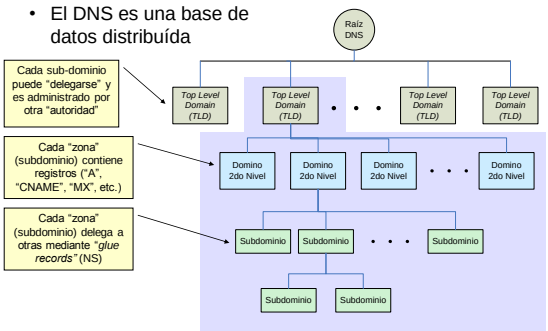
- Para que el *phishing* "funcione" hacen falta:
  - Un sistema comprometido donde alojar las páginas web que simulan al sitio "real"
  - Una forma de direccionar (nombre o IP), para dirigir a los usuarios al mismo
    - En general, las IPs de los sistemas mas frecuentemente comprometidos son variables, 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
- Propósito básico:
  - Traducir números IP en nombres textuales mas amigables para los usuarios "humanos" de la red
- Propósitos adicionales:
  - Soporte a diferentes servicios a dar sobre la red (directorio de servicios)
    - Ejemplo: Correo electrónico
  - Sub-delegaciones de nombres
    - Zonas, autoridad
  - Resolución reversa
    - Reverso: correspondencia nombre -> número IP

DNS (II)

- El DNS es una base de datos distribuída



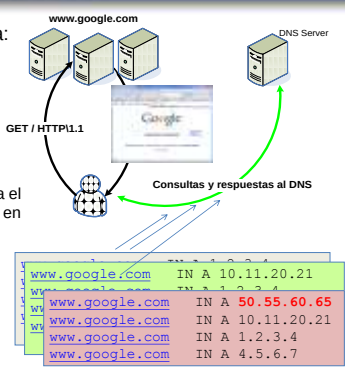
DNS (III)

- Estructura de los nombres de dominio:

- Comentarios:
  - Los niveles del árbol reflejan las delegaciones
  - El *root* del árbol presente de forma implícita
  - No hay restricciones a la cantidad de niveles
  - Los niveles superiores "**delegan**" hacia los inferiores

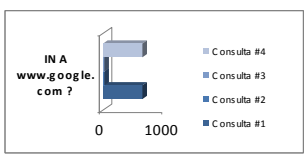
DNS Round Robin

- Técnica empleada para:
  - Balanceo de carga
  - Tolerancia a fallas
- Concepto:
  - Una consulta por un nombre devuelve varios registros
  - El servidor DNS permuta el orden de estos registros en respuestas siguientes
- Problemas:
  - Falta de *feedback* de servicios a DNS
  - Tiempo de reacción limitado por TTL de los registros



Time-to-Live

- Cada consulta al DNS es "costosa"
  - Consulta a servidores remotos
  - Consultas recursiva
- Los resultados se almacenan en *caché* local
- ¿Por cuánto tiempo? *Time-to-Live*
- Típicamente
  - 86400 segundos (1 día)



El "Problema" (para el atacante)

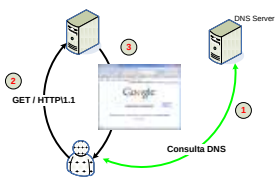
- Bloqueos
  - Un sitio de phishing o similar, "tradicional" es muy sencillo de bloquear una vez detectado
    - Basta con eliminar el sistema comprometido que aloja las páginas fraudulentas
  - La distribución de software en la Botnet también puede ser bloqueada de manera completa si se detecta el sistema central
  - Los administradores de redes en general toman acciones inmediatas contra sitios de phishing y similares bloqueándolos
- *¿Como puedo dotar de alta disponibilidad a mi botnet?*

La "Solución" (para la misma…)

- Eliminar los puntos únicos de falla
  - Web Server
    - Sistema comprometido donde se aloja el phishing
  - Resolución de nombres
    - a donde se apunta el phishing
- *Fast Flux Service Networks*
- Modos
  - *Single flux:* Servidor web
    - Servidor web distribuido, no ya un único sistema
      - Registros "A" en *round robin*
  - *Double flux:* Resolución de nombres
    - Resolución de nombres distribuída
      - Registros "NS" variables

Anatomía de una *FFSN*

- Acceso web "*normal*"



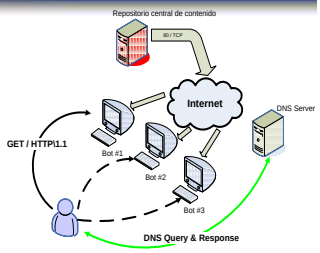
- Etapas
  1. Consulta al DNS por "A" de www.google.com
  2. Envía pedido HTTP al servidor web
  3. Obtiene la página buscada

Anatomía de una *FFSN:* Tipos

- *Single Flux*
  - Múltiples servidores web
    - Alojados en sistemas comprometidos (botnets)
  - Servidores DNS limitados
    - Alojados en proveedores de DNS "usuales"
      - Deben permitir configurar dinámicamente registros "A" con TTLs pequeños
- *Double Flux*
  - Múltiples servidores web
  - Múltiples servidores DNS
    - Proveedor de DNS debe además permitir la configuración dinámica de registros "NS"

Anatomía de una *FFSN: Single Flux*

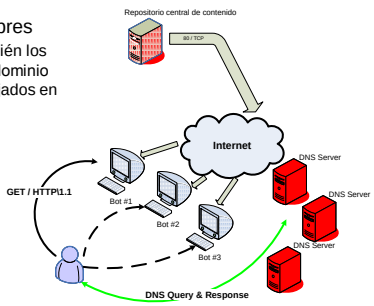
- ¿En que se diferencia del caso normal?
  - Múltiples registros "A" devueltos por el DNS
  - TTLs muy pequeños
  - Los "servidores" son en general computadores personales comprometidos
  - Registros "A" van cambiando con el tiempo
- Servidores DNS similares al caso "normal"
  - Pocos registros
  - Asociados a un proveedor



- Observaciones
  - Contenido entregado desde un sitio central
    - Facilita gestión

Anatomía de una *FFSN: Double Flux*

- El *double flux* agrega "redundancia" a la resolución de nombres
  - En este caso, también los registros "NS" del dominio asociado están alojados en bots y varían



Detección de *FFSNs*

- Holz et al [1] proponen un criterio de *scoring* para detectar FFSNs
- Posibles parámetros:
  - ***nA***: el número de registros "A" devuelto por la consulta
  - ***nNS***: el número de registros "NS" devueltos por la consulta
  - ***nASN***: el número de sistemas autónomos diferentes representados en los registros "A"

Detección de *FFSNs* (2)

- Otros criterios:
  - Nombres reversos de las IPs devueltas en la consulta pertenecientes a redes de clientes ADSL, dialup o similares
  - Variaciones temporales nA o nNS
    - Respuesta a eliminaciones de nodos
  - TTLs en los registros pequeños
- Software
  - FFDetect
    - Biblioteca Java, Universidad de Wellington, *Open Source*
  - ffdetect.pl
    - Script Perl, CSIRT Antel, *Open Source*

Ejemplo de una *FFSN* detectada

- Dominio "81dns.ru" (salida de 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.
```

Ejemplo de una *FFSN* detectada (2)

- Reversos de “81dns.ru” (Registros “A”)

```
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 d14-69-151-27.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-b7d1e155.82-6-64736c12.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.
```

Conclusiones

- Las FFSNs:
  - Dan redundancia y estabilidad a redes para entrega de contenido dudoso
    - Phishings y otros fraudes
    - Venta de productos famacéuticos, etc.
  - Proveen de una capa adicional de anonimización a quienes operan estas redes
    - Difícilmente se puedan hallar logs en los PCs comprometidos (bots) que actúan de servidores web
  - Desde el punto de vista del ISP se debe ser cauteloso con las herramientas de gestión de DNS automatizadas de las que se proveen a los clientes
- Hace falta más investigación
  - Formas de detectar y de eliminar

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

¡Muchas gracias por su atención!

ANTEL

CSIRT

¡Muchas gracias por su atención!

ANTEL

CSIRT

¡Muchas gracias por su atención!

ANTEL

CSIRT

Amenazas en la Web

- Algunas amenazas…
  - Envío de correo electrónico no solicitado *(spam)*
  - Ataques de denegación de servicio distribuidos
  - *Phishing*
  - Instalación de "*adware*"
  - "*Sniffing"* de tráfico
  - "*Keylogging"*
    - Guardar las "teclas" pulsadas por el usuario y enviar esa información al "*bot herder*"
  - *"Click Fraud"*
    - Generación de clicks fraudulentos a herramientas de promoción en Internet (Google, Yahoo)
- **En general [el atacante] necesita alguna infraestructura**
  - Páginas de log in; agentes de recolección de datos; envíos de correo masivos

Amenazas en la Web