رئوس مطالب

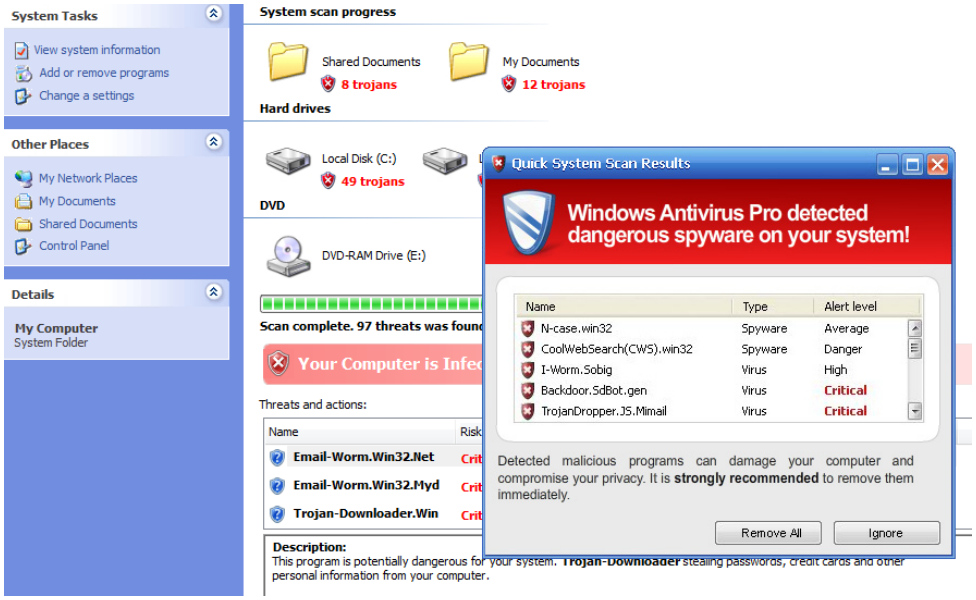
- مقدمه
- تعریف Botnet
  - روش های آلوده سازی
  - مکانیزم های C&C
- انواع Botnet
- تکنیک های پیشرفته Botnetها
- گرایشات جدید

مقدمه

- کرم های کامپیوتری قابلیت پخش شدن دارند و می توانند در زمان کمی میلیون ها کامپیوتر را آلوده کرده و شبکه ها را از کار بیاندازند.
- نفوذگران از آلوده کردن سیستم های کامپیوتری چه سودی می برند؟!
  - به آسانی نمی توان این سیستم های آلوده را به پول تبدیل کرد!!
  - طبق بررسی های انجام گرفته botmasterها می توانند در هفته بیش از $10,000 درآمد داشته باشند.
- برای استفاده حداکثری از سیستم های آلوده شده، نفوذگران باید بتوانند آنها را کنترل کنند.
  - چگونه و به چه منظور؟!

مقدمه

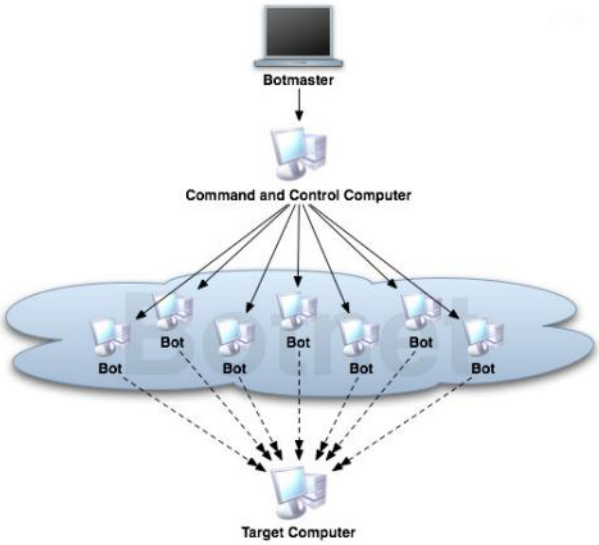
- بررسی درآمد حاصل از یک بات نت: KOOBFACE
  - از June 23, 2009 تا June 10, 2010
  - کل درآمد: 2,067,682$
  - میانگین روزانه: 5,857$
  - ۵۰.۳٪ از درآمد از طریق FAKE AV
  - ۴۹.۷٪ از درآمد از طریق PPC



Fake AV

مقدمه

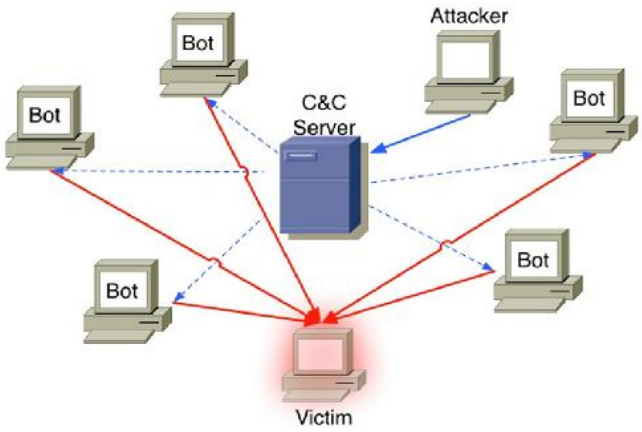
- نفوذگران با کنترل سیستم های آلوده می توانند حملات و اعمال غیر-قانونی بسیاری انجام دهند.
  - حملات DDoS
  - ارسال هرزنامه (Spam)
  - دزدی اطلاعات و هویت
  - تقلب در کلیک کردن (Click fraud)
  - حملات Phishing
  - ...



- برای این منظور، نفوذگران به یک ساختار C&C نیاز دارند.

Botnet چیست؟

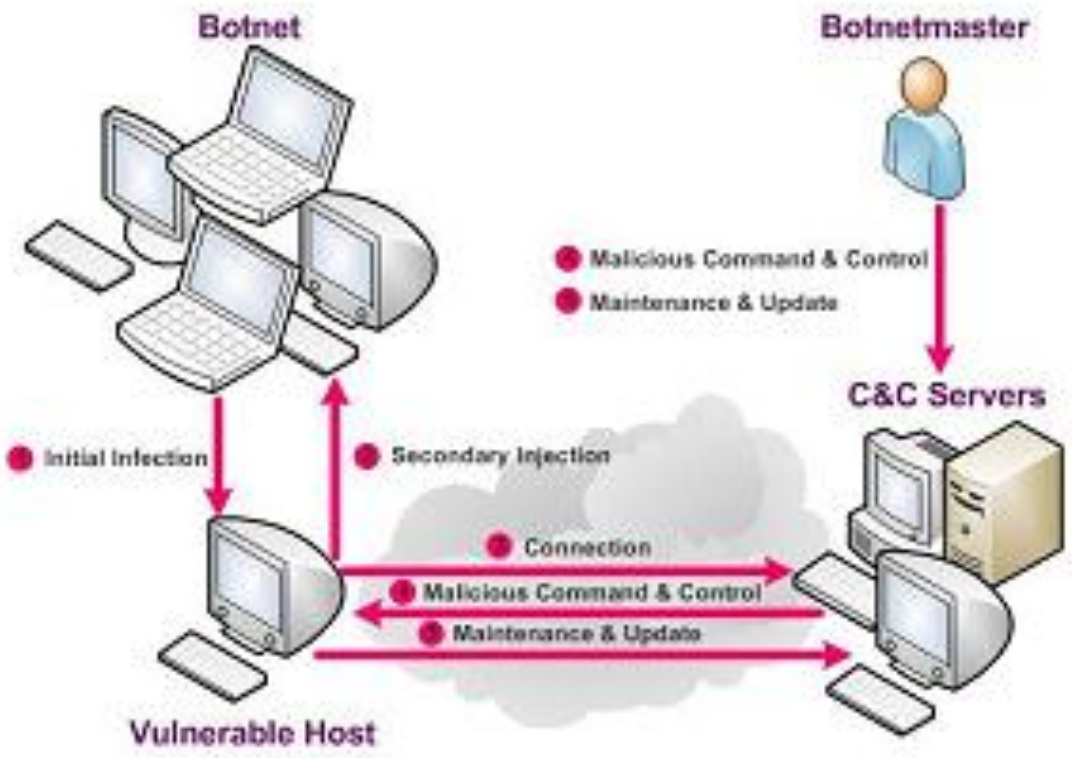
- یک Bot یا Zombie سیستمی آلوده شده است که می تواند توسط نفوذگر و از راه دور کنترل شود.
- Bot ها سه ویژگی اصلی دارند:
  - قابلیت کنترل از راه دور
  - قابلیت اجرای دستورات مختلف
  - مکانیزم گسترش به منظور تکثیر



- Botnet شبکه ای است شامل تعداد زیادی از سیستم های آلوده شده (bot) که توسط نفوذگر کنترل می شود.

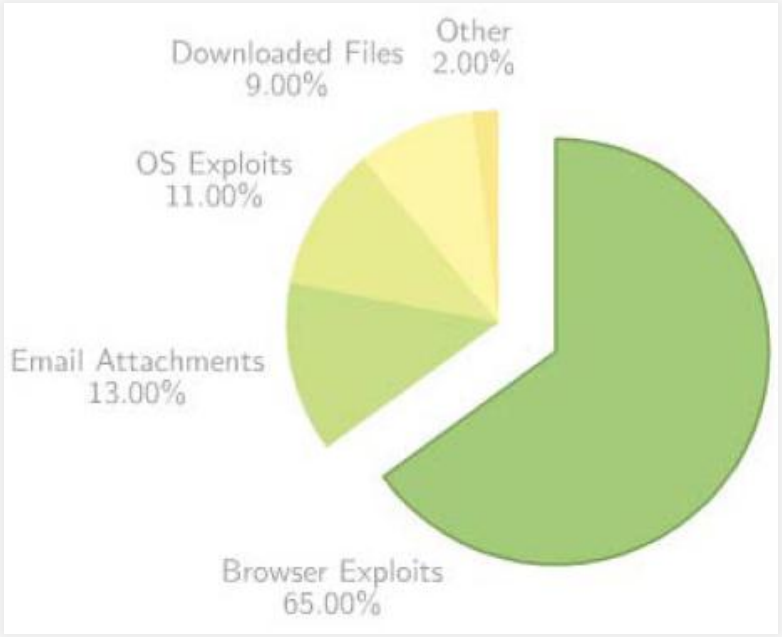
چرخه زندگی Botnet

- آلوده سازی اولیه
- تزریق ثانویه
- ارتباط با C&C
- ارسال دستورات C&C
- نگهداری و بروز رسانی



روش های آلوده سازی

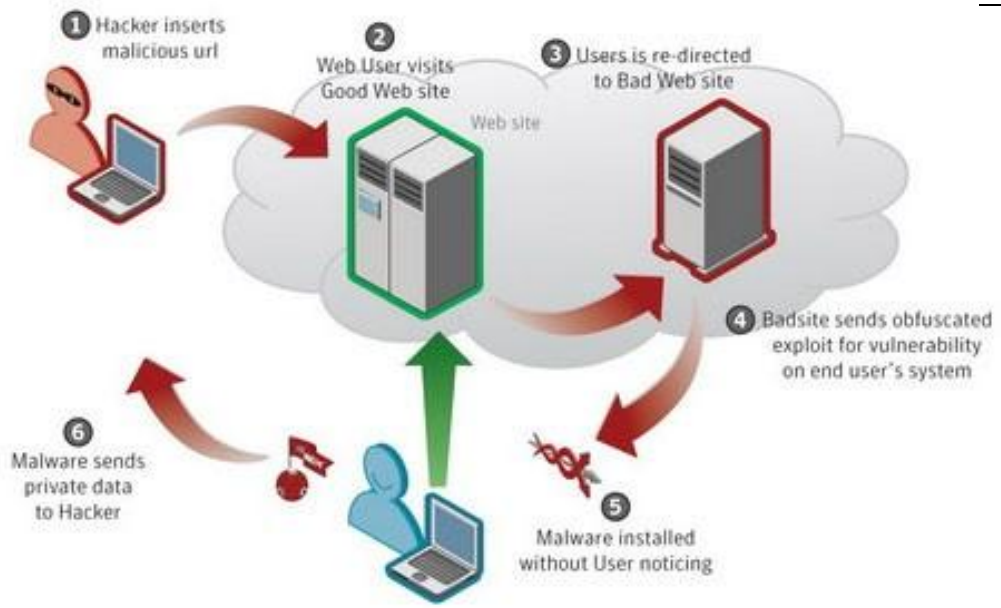
- روش های مهندسی اجتماعی (Social Engineering)
  - معمولاً ضعیف ترین حلقه در زنجیره امنیتی، عوامل انسانی می باشد!



متدهای آلوده سازی (منبع: S21sec)

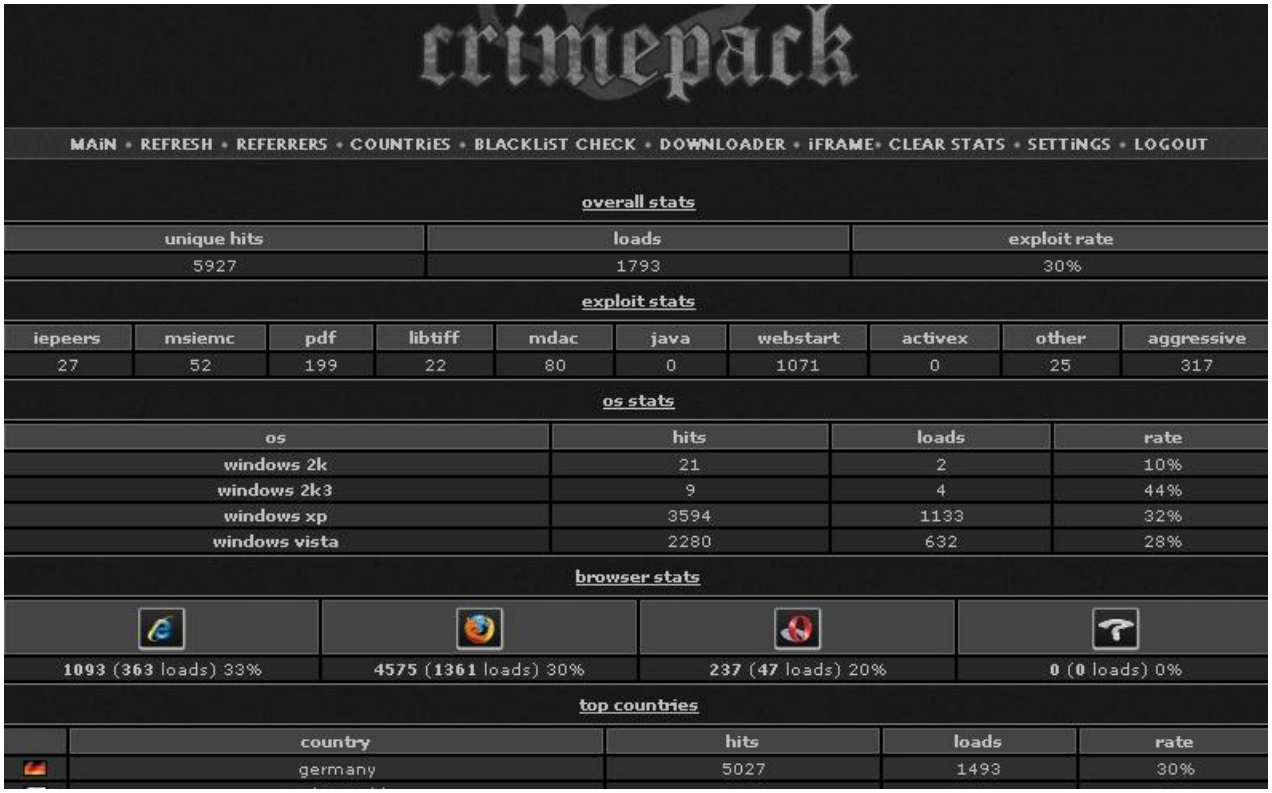
روش های آلوده سازی

- آسیب پذیری برنامه های کاربردی سمت کلاینت
  - حملات Drive-by Download
    - سوء استفاده از آسیب پذیری های موجود در مرورگرهای وب، پلاگین های نصب شده (مانند Adobe Flash) و یا برنامه های کاربردی سمت کلاینت برای نفوذ به سیستم هدف و دانلود بدافزار بدون اطلاع کاربر!



Exploit Packs: روشی برای ایجاد Botnet

- مجموعه ای از کدهای اکسپلویت (آسیب پذیری های سمت کلاینت) که بر روی وب میزبانی می شود و می تواند کاربران بازدید کننده سایت را آلوده کند.



مکانیزم های Command & Control

- یکی از مهمترین اجزاء هر Botnet، ساختار C&C آن می باشد.
- در صورتی که دستورات تعریف شده در bot نیاز به بروز رسانی داشته باشد، مدیر botnet می تواند این دستورات را بروز رسانی کند.
- علاوه بر انعطاف پذیری و قابلیت هایی که C&C فراهم می کند، این جزء از botnet، حساس ترین حلقه این سیستم نیز می باشد.
  - برای نمونه با از کار انداختن C&C، نفوذگر دیگر کنترلی بر bot ها ندارد و عملاً botnet از کار می افتد.
- به همین دلیل مدیران botnetها همواره در جستجوی راه های جدید برای پنهان-سازی C&C و افزایش قابلیت اطمینان این ساختار هستند.

مکانیزم های Command & Control

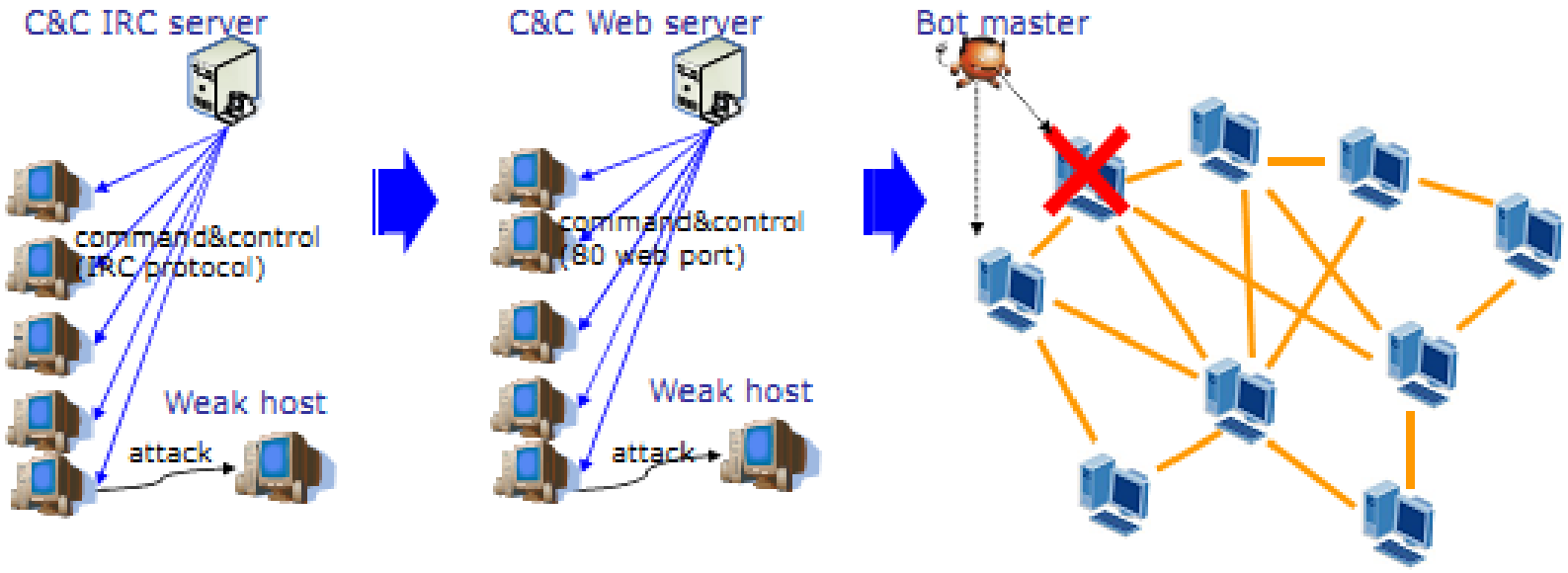
- مدیران botnet با استفاده از روش های مختلفی سعی در ایجاد C&C قابل اعتماد دارند.
  - ساختار P2P در مقابل ساختار متمرکز
  - سرویس Fast-Flux
  - Domain-Flux – الگوریتم های تولید دامنه (DGA)
  - روش های مقابله با آنالیز (در فایل باینری botها)
- در مقابل، متخصصان امنیتی هم با استفاده از روش های مختلفی سعی در شناسایی و از کار انداختن botnet ها دارند.
  - Take-down هماهنگ

انواع Botnet

- عموماً Botnet ها را بر اساس نوع ساختار C&C آنها به دو دسته کلی متمرکز و غیر متمرکز تقسیم می کنند.
- مکانیزم های C&C متمرکز
  - با استفاده از روش push، مثل IRC
  - با استفاده از روش pull، مثل HTTP
- مکانیزم های C&C غیر متمرکز
  - روش P2P

- به دلیل مشکلات روشهای متمرکز و از بین بردن single point of failure، مدیران Botnet ها پروتکل های P2P را جایگزین پروتکل IRC و HTTP کردند.

انواع Botnet



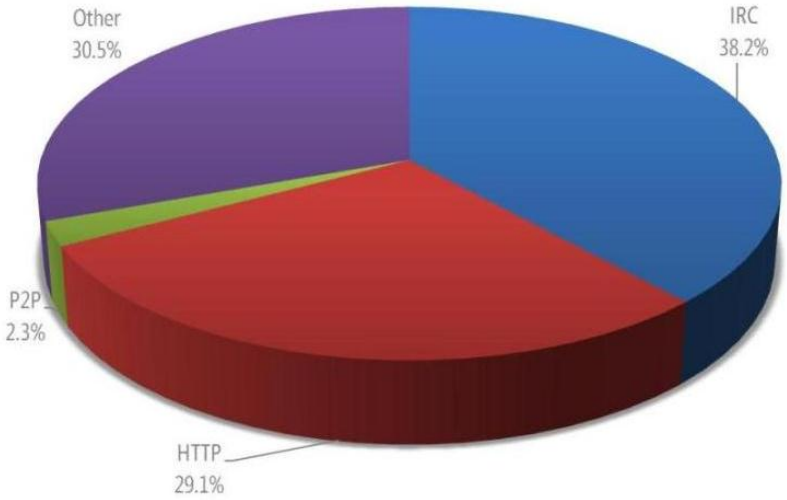
- Centralized control
- IRC Botnet

- Centralized control
- Use Web protocol
- HTTP Botnet

- Distributed control
- P2P Botnet

انواع Botnet

- با وجود مزایای پروتکلهای مختلفی مانند HTTP و P2P، هنوز هم درصد زیادی از Botnet ها از پروتکل IRC به عنوان C&C استفاده می کنند.
- گزارش مایکروسافت از مکانیزم های C&C استفاده شده توسط Botnet ها در نیمه دوم سال 2010:



تکنیک های پیشرفته بات نت ها

- Obfuscation
  - مبهم سازی Bot: استفاده از Crypter / Packer و استفاده از تکنیک هایی برای مخفی شدن از دید آنتی ویروس ها و دیباگرها!
- کشف ماشین های مجازی (Anti-VM)
- کشف Sandbox
- کشف Honeypot

تکنیک های پیشرفته بات نت ها

- Domain-Flux
  - تولید نام های دامنه تصادفی
  - نیاز استفاده از این تکنیک:
    - محققان امنیتی می توانند سرورهای C&C و میزبان اکسپلویت را Take-down کنند.
    - آدرس های IP استاتیک را به راحتی می توان blacklist کرد.
      - معرفی دامنه های Fast-Flux...
    - آدرس های DNS استاتیک نیز می توانند Take-down شوند.
      - معرفی Domain-Flux...!
  - نمونه ای از بات نت ها که از این تکنیک استفاده می کنند:
    - Conficker، Torpig و ...

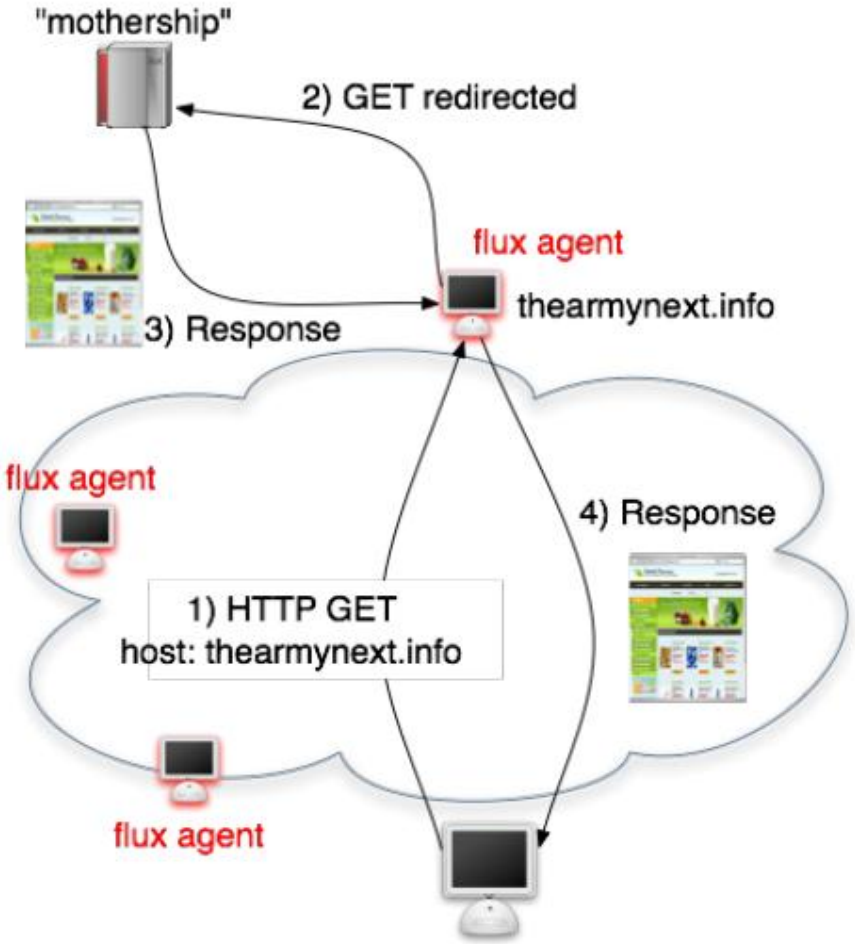
تکنیک های پیشرفته بات نت ها

- Domain-Flux
  - Bot ها به صورت دوره ای نام های دامنه جدیدی برای سرورهای C&C یا میزبان اکسپلویت تولید می کنند.
  - الگوریتم های تولید دامنه (DGA)
    - معمولاً به عنوان ورودی اولیه از زمان محلی سیستم استفاده می شود.
    - برای تکمیل آن می توان از Twitter API برای بیرون کشیدن کاراکترهایی از رایج ترین عناوین مورد جستجو قرار گرفته استفاده کرد.
  - Botmaster باید یکی از این دامنه های تولید شده را ثبت کند و به درستی به botها پاسخ دهد، تا به عنوان C&C معتبر شناخته شود.
  - در این صورت محققان برای take-down کردن Botnet باید تمام دامنه ها را ثبت کنند.

تکنیک های پیشرفته بات نت ها

- سرویس شبکه Fast-Flux (FFSN)
  - از این تکنیک به منظور مخفی کردن سایت های phishing و میزبان بدافزار در پشت شبکه ای از سیستم های آلوده شده – که مانند proxy عمل می کنند – استفاده می شود.
  - بعضی از بات نت های P2P از این سرویس به عنوان یک راه ارتباطی پشتیبان استفاده می کنند (Backup C&C) و بعضی از بات نت های متمرکز نیز به عنوان C&C اصلی.
  - خصوصیات:
    - یک تکنیک DNS
    - تعداد بسیار زیادی IP (صدها یا هزارها)
    - تغییرات دائم و سریع
    - Round-robin IP addresses + Short time-to-live (TTL)

تکنیک های پیشرفته بات نت ها – FFSN



فرآیند دریافت محتوای میزبانی شده بر روی سرویس شبکه Fast-Flux

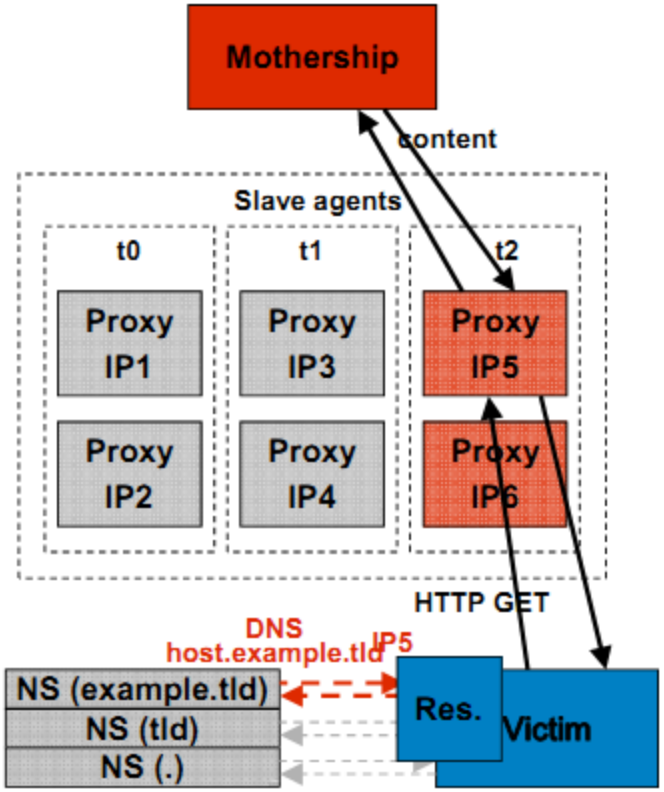
تکنیک های پیشرفته بات نت ها – FFSN

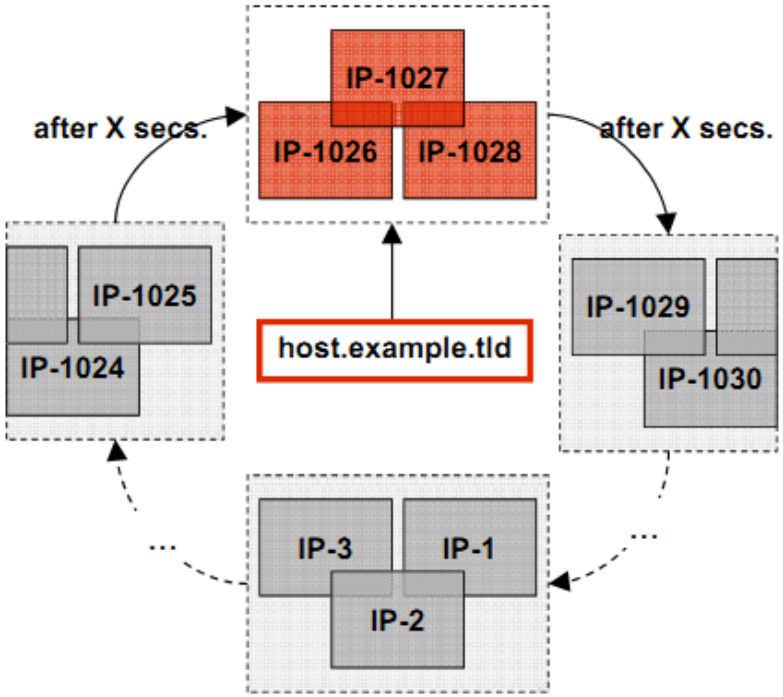
- درخواست داده شده برای دامنه Fast-Flux زیر تعدادی از IP های سیستم های آلوده (flux agents) را برگردانده است.
- در درخواست دوم (بعد از expire شدن TTL) مجموعه کاملاً متفاوتی از IP ها برگردانده شده است.

```
;; ANSWER SECTION:
thearmynext.info.       600     IN      A       69.183.26.53
thearmynext.info.       600     IN      A       76.205.234.131
thearmynext.info.       600     IN      A       85.177.96.105
thearmynext.info.       600     IN      A       217.129.178.138
thearmynext.info.       600     IN      A       24.98.252.230
```

```
;; ANSWER SECTION:
thearmynext.info.       600     IN      A       213.47.148.82
thearmynext.info.       600     IN      A       213.91.251.16
thearmynext.info.       600     IN      A       69.183.207.99
thearmynext.info.       600     IN      A       91.148.168.92
thearmynext.info.       600     IN      A       195.38.60.79
```

تکنیک های پیشرفته بات نت ها – FFSN





منبع: CERT Polska

گرایشات جدید

- Opt-in Botnet
- روش های ارتباطی جدید برای C&C
  - استفاده از شبکه های اجتماعی به عنوان C&C
    - Facebook، Twitter، ...
  - استفاده از Steganography
  - پروتکل های دیگر مانند DNS، SIP و ...
- Mobile Botnet
  - ظهور بدافزارهای قابل کنترل بر روی پلتفرم دستگاه های سیار
    - بد افزارهای Android