بات نت
(Botnet)

تعاریف

- Bot
  - برنامه های خود مختاری که به صورت خودکار کارهایی را انجام می دهند.
- Botnet
  - شبکه ای از برنامه های خود مختار که توانایی انجام دستورات را دارند.

پدیدار شدن Botnet

- ۲۰۰۳
  - ۸۰۰ هزار تا ۹۰۰ هزار هاست آلوده، ۱۰۰ هزار Bot در هر Botnet
- ۲۰۰۶
  - ۵ میلیون Bot، Botnetهای کوچکتر
    - هزاران Bot به جای صدها هزار Bot
    - دلایل: اقتصادی، مدیریت کاراتر و راحتتر
- هدف: کسب منفعت به جای آسیب رسانی

فعالیت های Botnet

- Distributed DoS
- Spamming
- Click fraud
- فریبکاری در بازی ها و رأی گیری های آنلاین

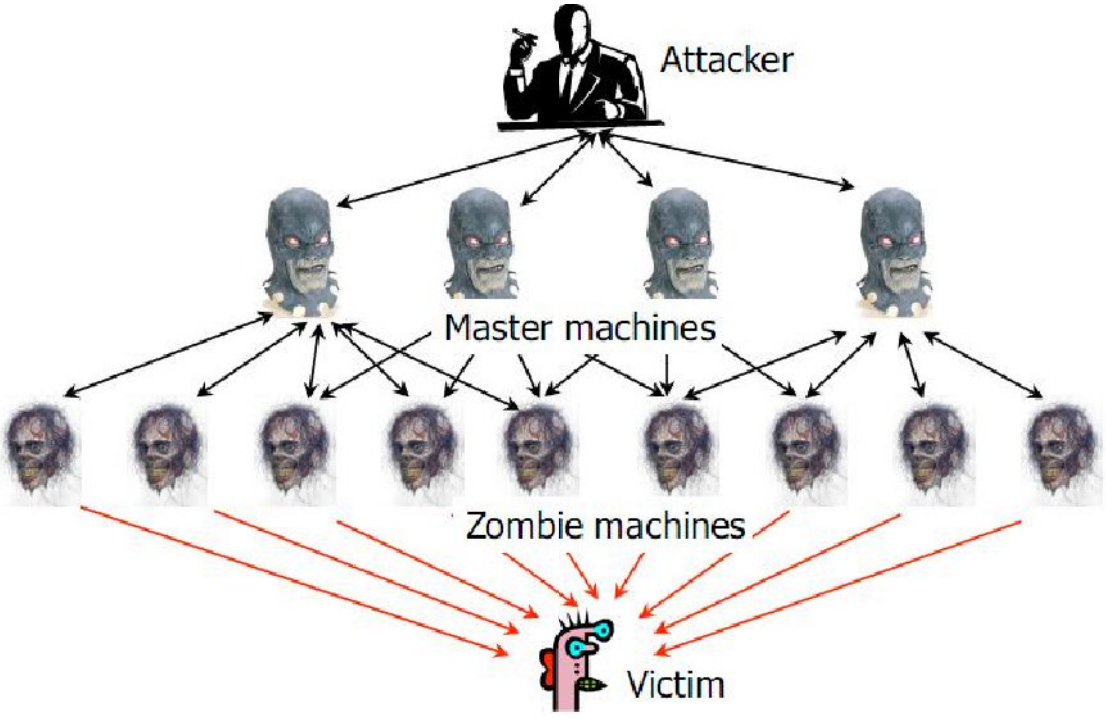
Denial of Service (DoS)

- هدف: از توان انداختن ماشین تا نتواند به کلاینت های مجاز سرویس دهد.
- DoS اصولاً از پروتکل های شبکه سوء استفاده می کند:
  - Smurf: ارسال ICMP echo به تمام هاست ها با جعل آدرس مبدأ و گذاشتن آدرس قربانی به عنوان آدرس مبدأ
  - Ping of death: ارسال بسته های ICMP با payload بیش از 64k باعث از کار افتادن نسخه های قدیمی ویندوز میشد.
  - SYN Flood: ارسال بسته های SYN با آدرس مبدآ جعلی
  - UDP Flood: ارسال بسته های UDP برای مصرف کردن پهنای باند قربانی

Distributed Denial of Service (DDoS)

- Botnet ای از zombieها
  - معماری چند لایه: بعضی از zombieها به عنوان Master انتخاب می شوند تا دیگر zombieها را کنترل کنند.
- دستور به zombieها برای ترتیب دادن یه حمله هماهنگ
  - احتیاجی به spoofing نیست.
  - هنگام حمله SYN Flood، استفاده از SYN Cookies فایده ای ندارد.
- از کار انداختن قربانی با ترافیک حجیمی که از طرف هزاران هاست مختلف می آید.

معماری DDoS



Trin00

- آسیب پذیری سرریز بافر را لینوکس و سولاریس اسکن می کند.
  - wu-ftpd، statd، amd، ...
- نصب سرویس حمله با استفاده از دسترسی ریموت شل
- ارسال دستورات و تأیید هویت با پسورد به صورت plaintext
  - مهاجم به master: TCP و master به zombie: UDP
  - برای جلوگیری از شناسایی، سرویس در صورت اتصال فردی به آن همزمان با اتصال به master، اخطار می دهد.

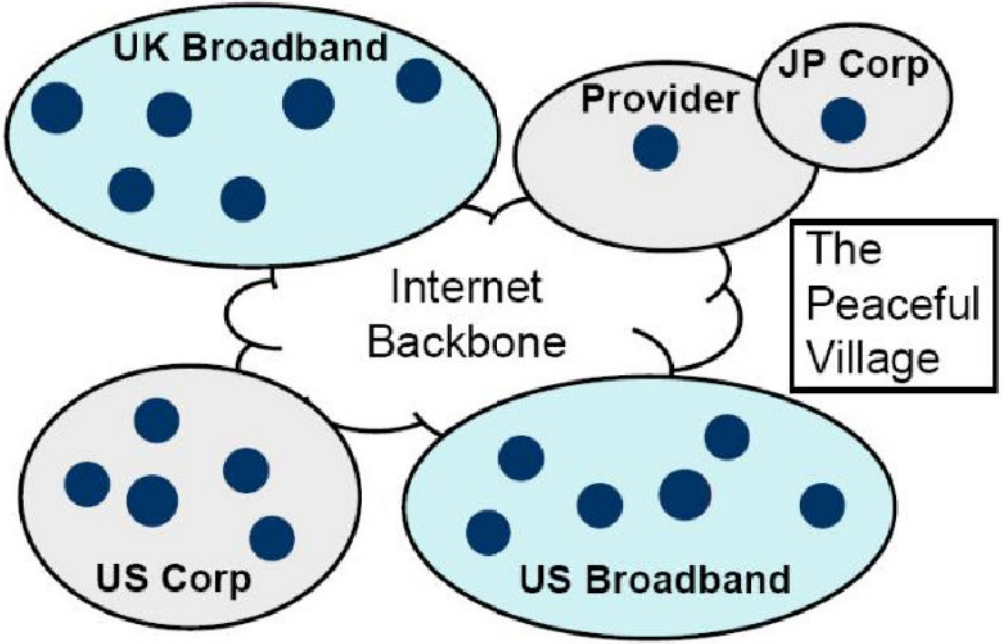
Agobot

- ۲۰ هزار خط کد C/C++
- کانال دستور و کنترل مبتنی بر IRC
- دارای ابزار اسکن کردن و بردارهای انتشار متنوع
- توانایی انجام انواع حملات DoS Flooding
- استفاده از تکنیک های تغییر کد برای عدم شناسایی
- نصب sniffer، بستن پروسس آنتی ویروس ها و فیلتر کردن آدرس DNS سایت های آنتی ویروس ها

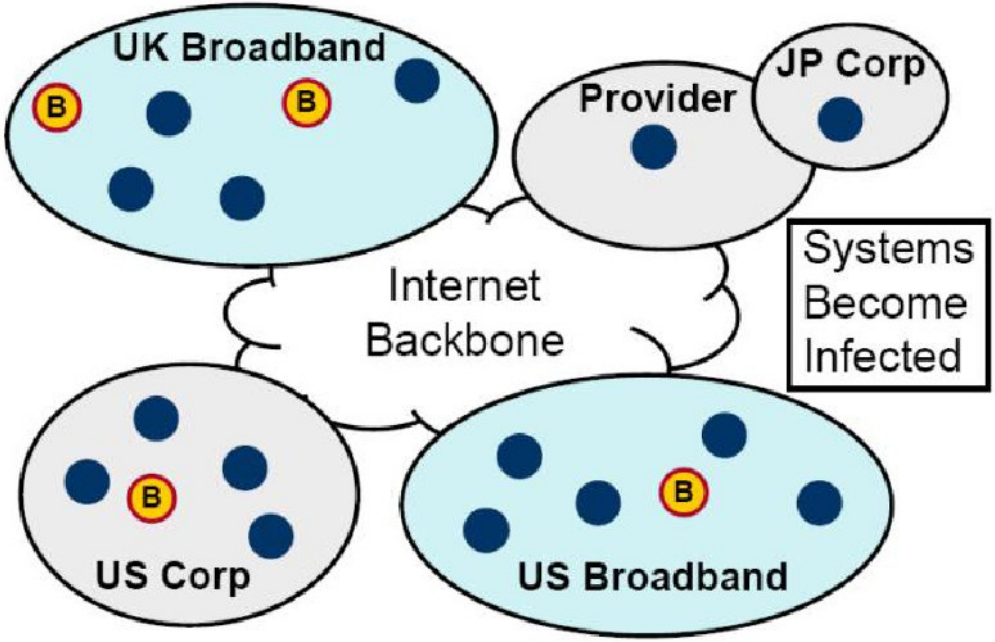
دیگر Botهای مدرن

- SdBot/SpyBot
  - غیر مخرب، ولی می توانند برای انجام اسکن کردن، sniffing و حملات DoS مجهز شوند.
- GT-Bot
  - اسکن کردن، DoS
  - آسیب پذیری های RPC و NetBIOS
  - ساده تر از Agobot (۳۰۰۰ خط کد C)
  - قابل گسترش
- روند: ترکیبی از bot، تروجان و کرم

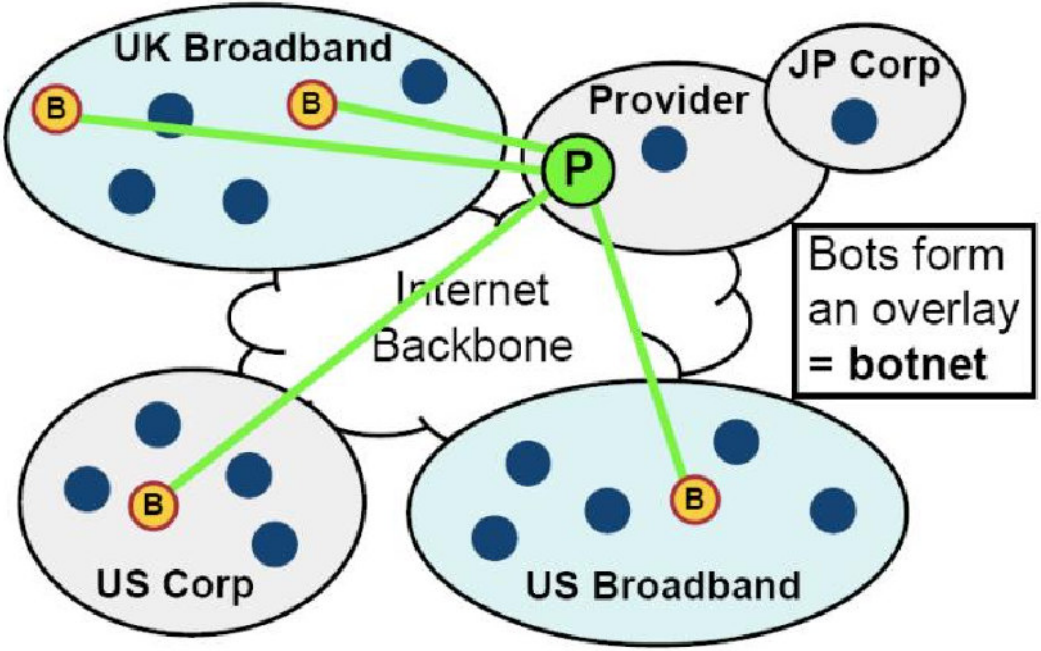
تولید Botnet (۱ از ۵)



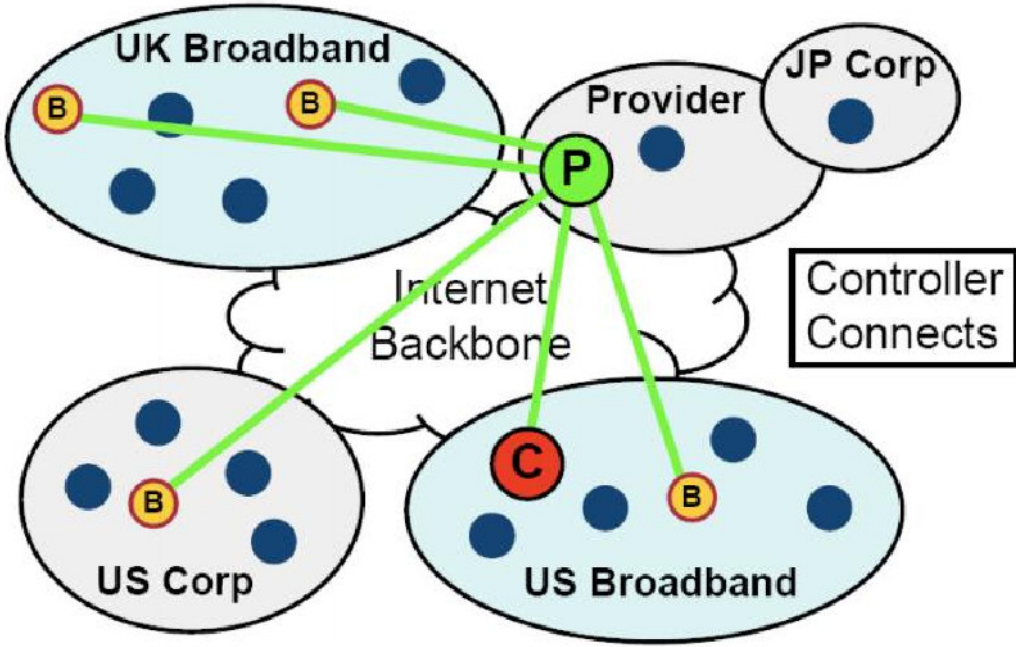
تولید Botnet (۲ از ۵)



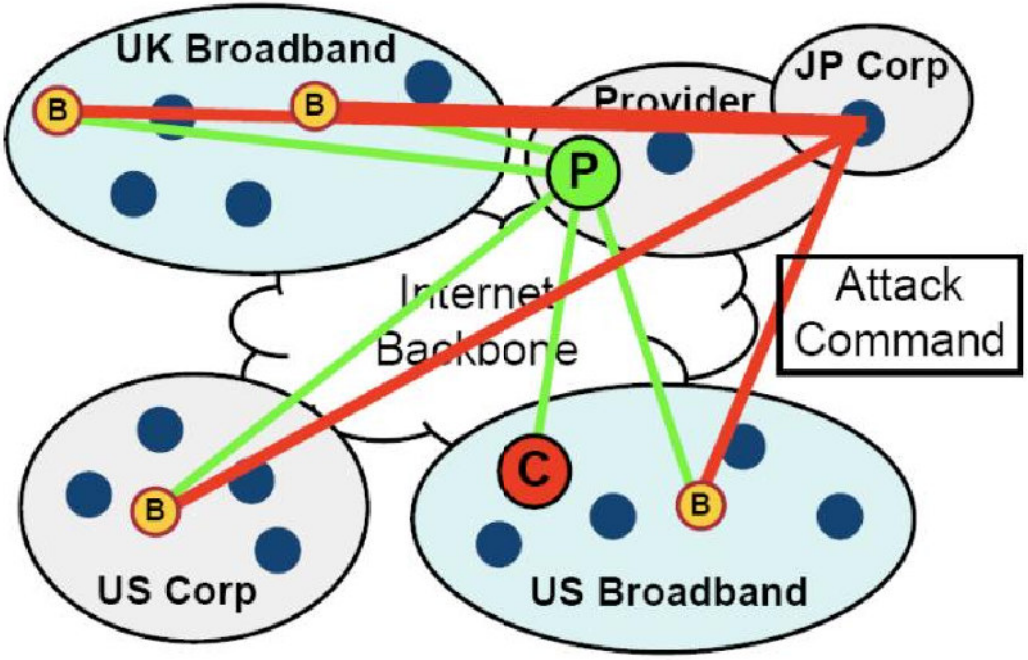
تولید Botnet (۳ از ۵)



تولید Botnet (۴ از ۵)



تولید Botnet (۵ از ۵)

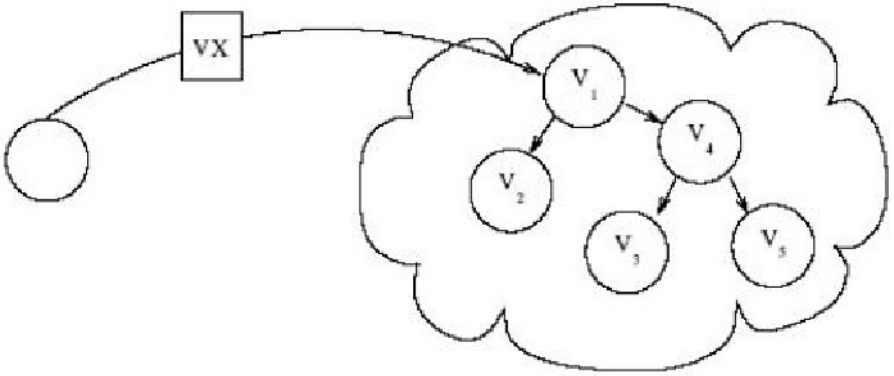


انتشار Botnet (استخدام Botهای جدید)

- ایمیل
  - احتیاج به تعامل با کاربر دارد، مهندسی اجتماعی
  - روشی راحت و همگانی
- instant message
  - مهندسی اجتماعی
  - انتقال فایل
  - آسیب پذیری ها
- سوء از استفاده از آسیب پذیری نرم افزارها از راه دور
  - احتیاجی به تعامل با کاربر نیست.

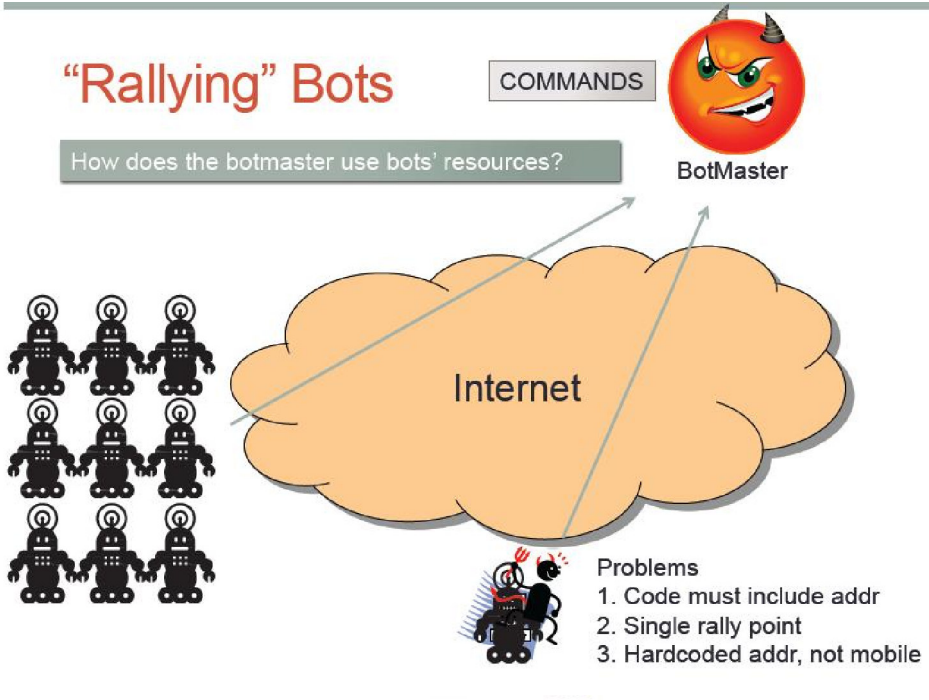
Rallying Problem

- چگونه Botهای یک Botnet را سازماندهی کنیم؟



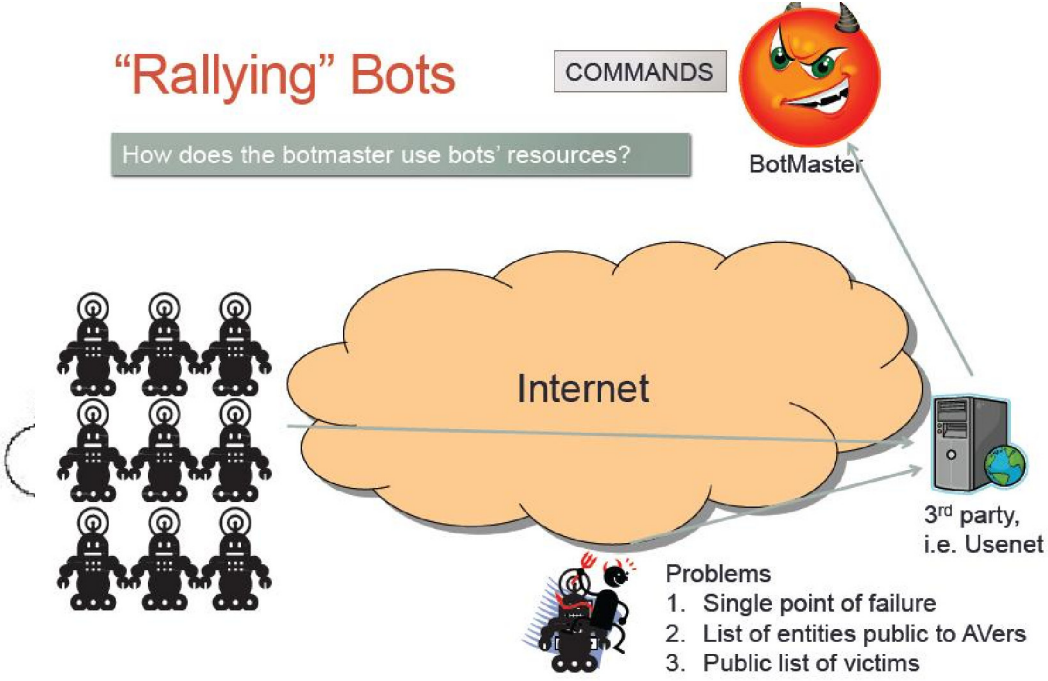
Rallying I

- Botها به طور مستقیم به مهاجم وصل شوند.



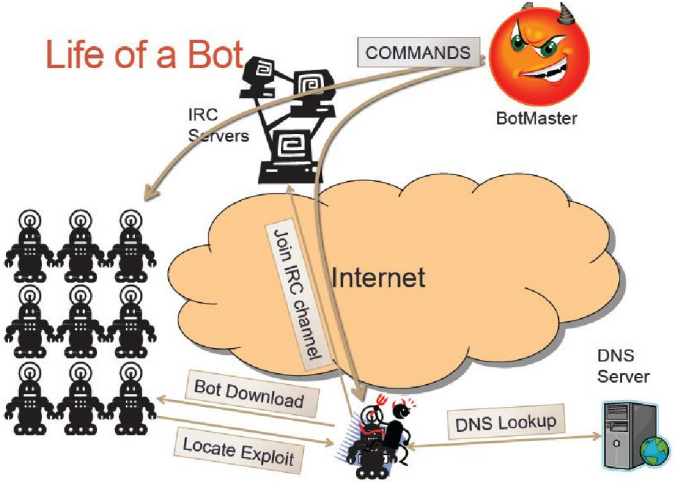
Rallying II

- Dynamic DNS Domain name



Rallying III

- DNS های توزیع شده
  - آدرس dns ها در کد های Bot ها وجود دارد
  - با اتصال به این DNS ها IP مربوط به Bot master یا IRC پیدا می شود.
  - به سختی قابل شناسائی است



انواع مرکز دستور و کنترل

- IRC
  - SdBot
- Http
  - Babox
- Peer to peer
  - Phatbot, نسل جدیدی از AgoBot

Bot/Botnet Measurement

- داده های کمی روی botnet موجود است.
- تعداد botnetها در حال افزایش است.
- تعداد bot در هر botnet در حال کاهش یافتن است.
  - در حال حاضر چند هزار bot

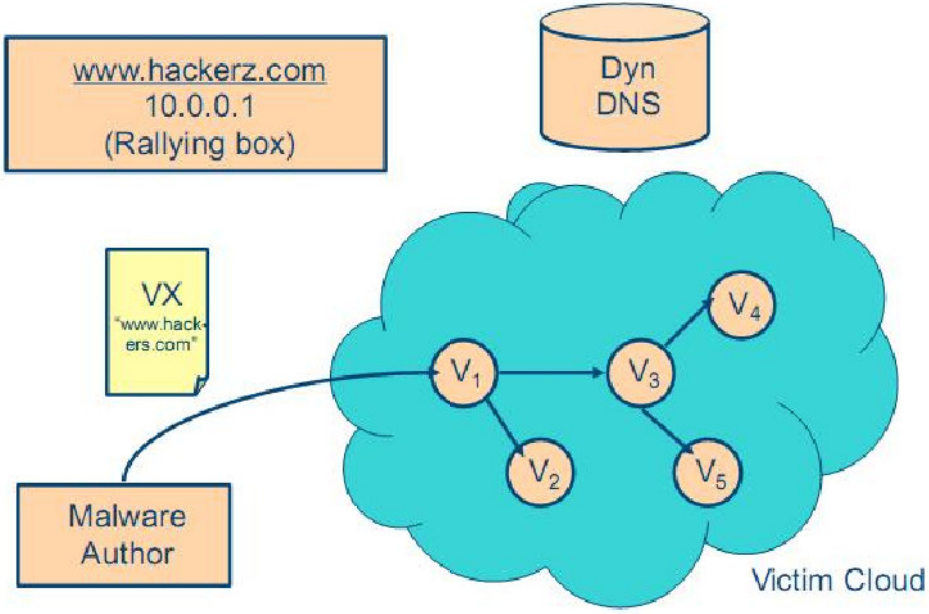
شناسایی Botها

- محافظت از سیستم ها برای جلوگیری از آلوده شدن
- شناسایی ارتباطات bot
  - ارتباطات بین bot و سرور دستور و کنترل
  - مانند IRC Botnets
    - پورت TCP ۶۶۶۷
    - مانیتور کردن IRC payload برای یافتن دستورات شناخته شده

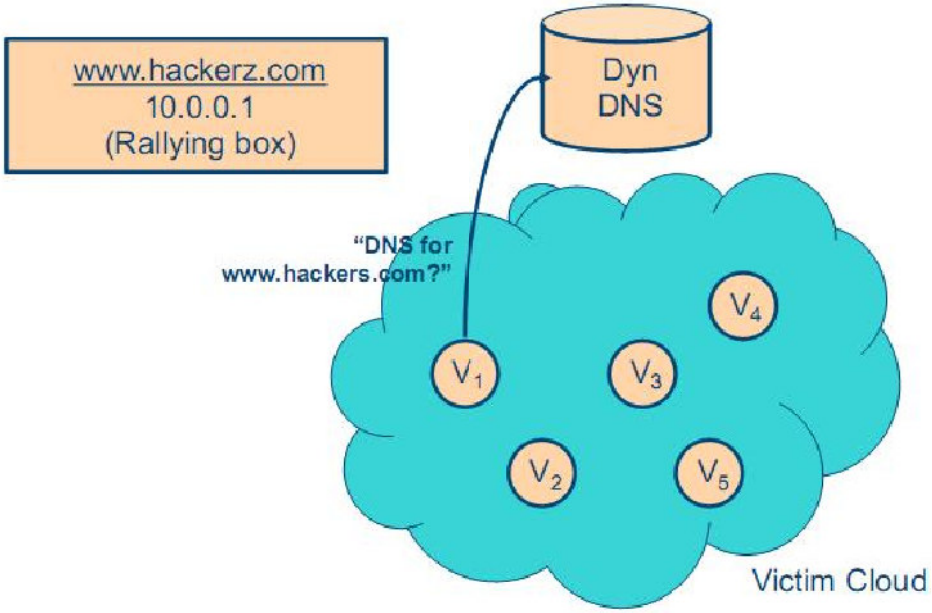
شناسایی Botها (ادامه)

- بررسی خصوصیات رفتاری
  - کلاینت های IRC که سریع پاسخ می دهند، ممکن است bot باشند.
    - Netflow های مربوطه را از ترافیک استخراج کنیم.
- دنبال کردن Botnet با استفاده از Honeypot
  - از Honeypot استفاده کنیم تا آلوده شویم.
  - یک bot جدید بسازیم و عضو botnet شویم.

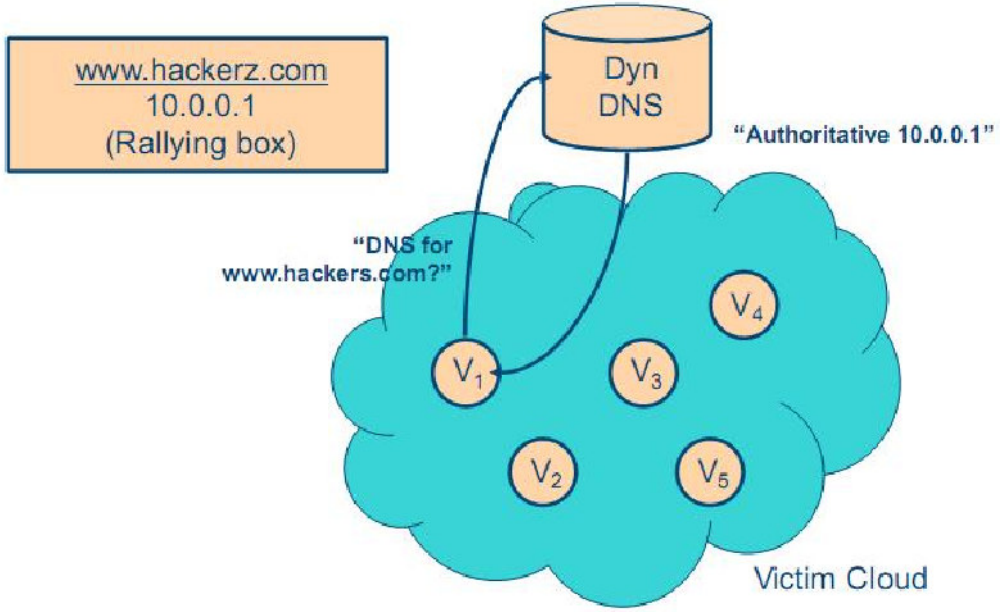
غیر فعال سازی Botnet با Sinkhole



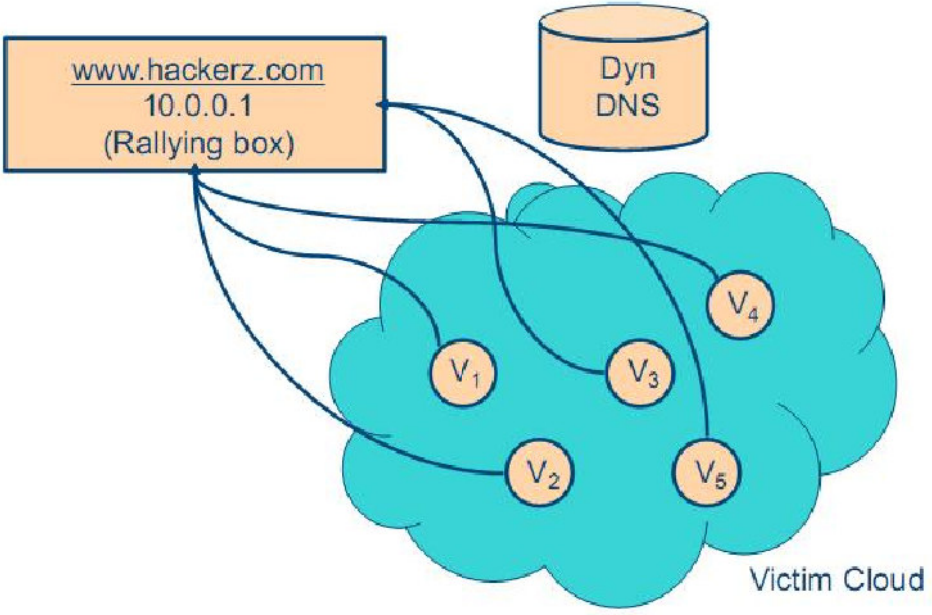
غیر فعال سازی Botnet با Sinkhole



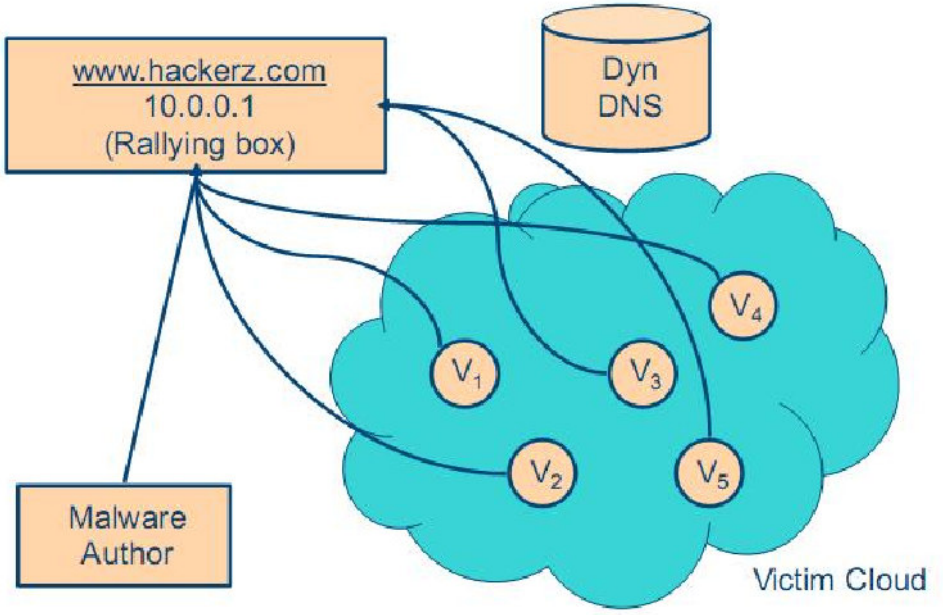
غیر فعال سازی Botnet با Sinkhole



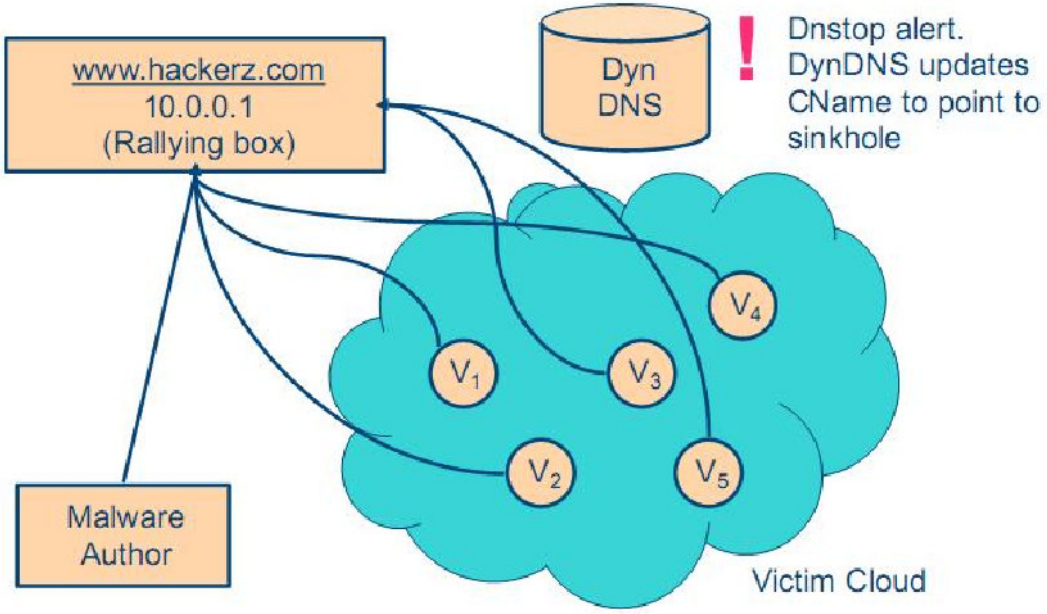
غیر فعال سازی Botnet با Sinkhole



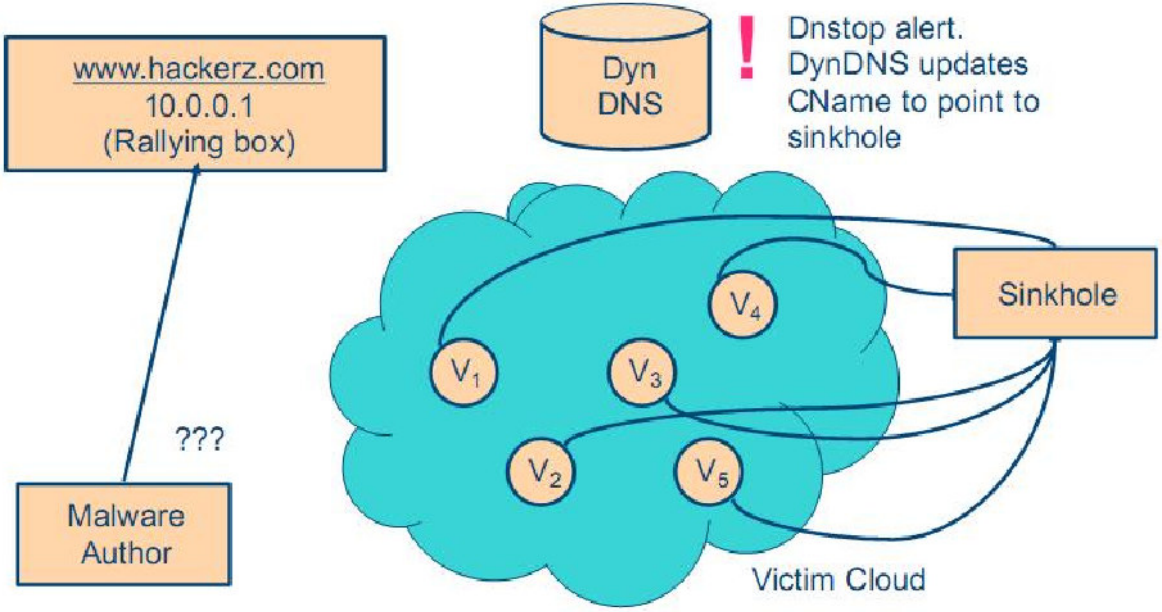
غیر فعال سازی Botnet با Sinkhole



غیر فعال سازی Botnet با Sinkhole



غیر فعال سازی Botnet با Sinkhole



نتیجه گیری

- امروزه Botnetها بزرگترین تحت امنیتی در اینترنت هستند.
  - منشأ بسیاری از حملات
- شناسایی و جلوگیری فقط در سطح شبکه امکان پذیر است.
  - شناسایی به طور مطلوب باید قبل از حمله صورت گیرد.