کرم
(Worm)

ویروس

- برنامه های آلوده
- هنگامی که برنامه اجرا می شود، آن برنامه عملیات نرمال خود را انجام می دهد.
- آن برنامه همچنین برنامه های دیگر را آلوده می کند.
- آن برنامه ممکن است که شامل payload اضافه ای باشد که کارهای دیگری انجام دهد.

کرم

- مانند ویروس است، ولی بین ماشین ها تکثیر می شود.
- بعضی از کرم ها کاملاً خودکار عمل می کنند. بعضی از آن ها احتیاج به دخالت کاربر دارند تا تکثیر شوند.
- بعضی از کرم ها از آسیب پذیری ها استفاد می کنند و بعضی از تکنیک های مهندسی اجتماعی

مشخصه های کر م ها

- روش پیدا کردن قربانی ها(Target finding)
- روش انتشار
- روش انتقال
- فرمت payload(برنامه های مخرب کرم)

روشهای پیدا کردن قربانی های جدید

- اسکن کور (Blind Scan)
  - اسکن تصادفی، پشت سر هم و جایگشتی
  - نرخ بالای ارتباط های نا موفق
  - امکان شناسائی با روش های Anomaly
  - در بعضی موارد با تکنیک هائی مانند اسکن شبکه محلی تقویت می شود.
  - عدم امکان در IPv6 و مشکل با NAT
- استفاده از لیست از پیش آماده شده
  - لیست هاست های قابل نفوذ قبلا تهیه می شود
  - امکان ذخیره در داخل کرم یا بار کردن از طریق شبکه
  - لیست های بزرگ مشکل حمل کردن در داخل کرم دارند و دانلود آنها نیز وقت گیر است
  - کرم Warhol ، با استفاده از لیست بزرگ در عرض ۵۱۱ میلی ثانیه حدود ۹۵٪ از لیست ۱۰۰۰۰۰۰ را الوده کرد

روشهای پیدا کردن قربانی های جدید(ادامه)

- مود غیر فعال
  - بعضی از کر مها منتظر می شوند تا یک هاست با نفوذ مورد نظر ارتباط برقرار کند سپس خود را در ان هاست کپی می کنند
  - کرم Gnuman یک نمونه است که در شبکه Gnutella منتظر یک query شده و سپس خود را تکثیر می کند.
  - کرم CRClean منتظر حمله CodeRed می شود تا حمله کننده را آلوده کند.
  - آرام باعِ الودگی می شوند و با روشهای anomaly یه سختی قابل شناسائی هستند.
- استفاده از ماشین های جستجو
  - بعضی از کزم ها از ماشین های جستجو مانند yahoo و google برای پیدا کردن هاست های قابل نفوذ استفاده می کنند.
  - کرم santy در گوگل دنبال وب سرور هائی می گردد که صفحات وب با محتوی "viewtopic.php" دارند.

رو شهای انتشار کرم ها

- Self-Carried
  - اکثر کرم ها خود راسا خود با بسته ها به قربانی جدید می فرستد.
- استفاده از یک کانال دوم
  - در بعضی موارد کرم به داخل ماشین قربانی رفته و با استفاده از backdoor کدهای خرابکار خود را دانلود می کند
- انتشار نهفته(Embedded)
  - برای انتشار کد های خود را به بسته های دیگر اضافه می کنند.
- استفاده از botnet ها برای تکثیر
  - کرم witty توسط botها منتشر می شوند.

روش های انتقال کرم ها

- کرم هایUDP
  - سرعت بالای انتشار
  - عرض باند محدود کنند است
  - این کرم ها برای منابع شبکه با هم رقابت می کنند
- کر م های TCP

- به دلیل نیاز به برقراری ارتباط 1. RTT سر بار زمانی بیشتری دارد. در این مدت ممکن است بلوک شوند
- زمان محدود کننده است.

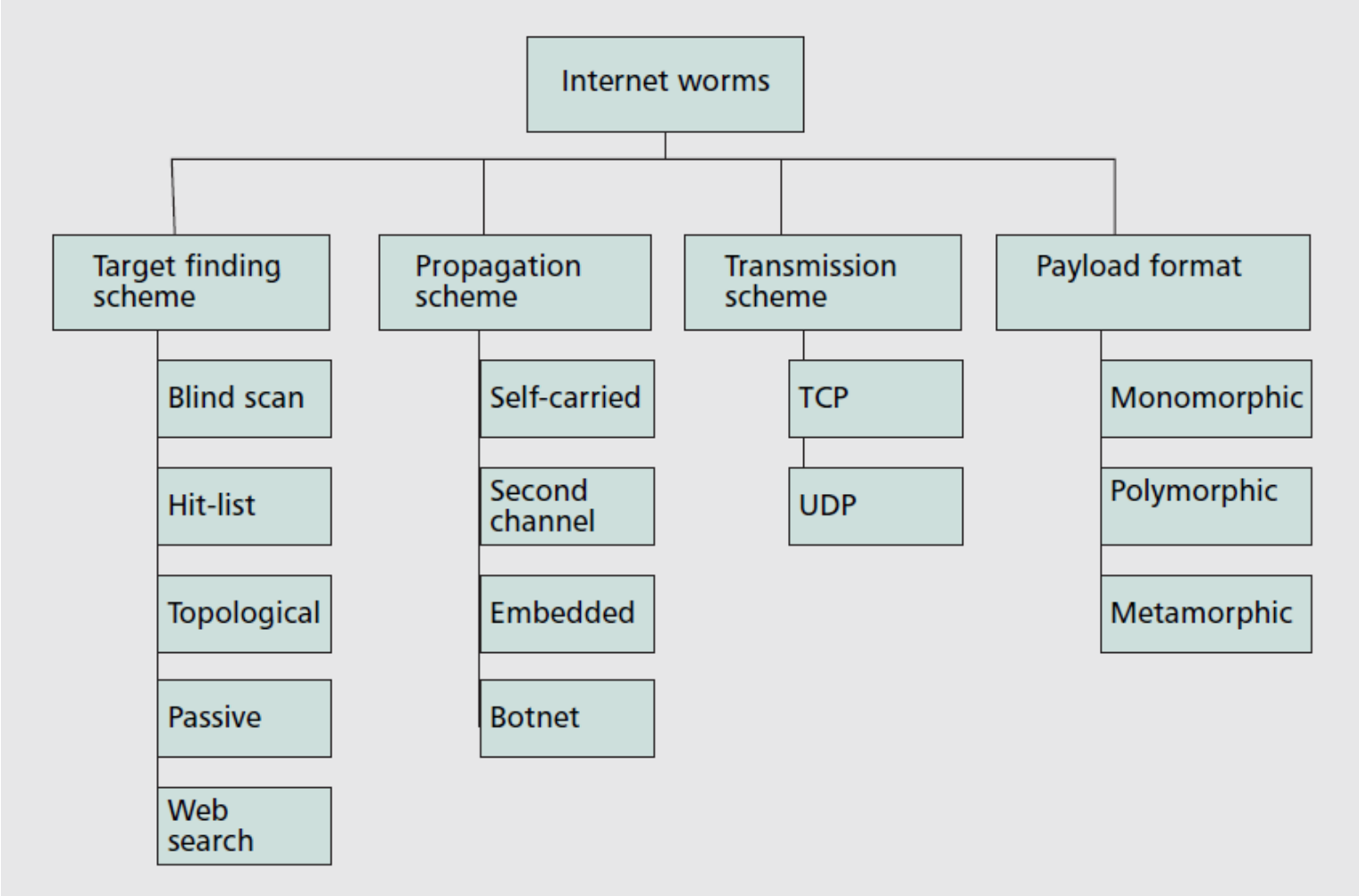
فرمت Payload در کرم ها

- منظور از payload کد برنامه کرم است
- کرم های تک ریختی(monomorphic)
  - یک برنامه با کد ثابت ، کرم برنامه خود را به قربانی منتقل می کند(کد برنامه یک signature برای کرم است)
  - بعضی ها با اضافه کردن(padding) داده های به دردنخور اندازه کد خود را تغییر داده سپس منتقل می کنند. کد اصلی باز ثابت است.
  - بعضی برنامه خود را به بخش های کوچکتر تقسیم کرده و سپس جدا جدا منتقل می کنند(برای جلوگیری از شناسائی signature based)
  - قابل شناسائی با روشهای signature based

فرمت Payload در کرم ها(ادامه)

- کرم های چند ریختی(Polymorphic)
  - بعضی از کرم ها با استفاده از تکنیک های scrambling به صورت پویا شکل کد را تغییر می دهند.
  - عملکرد همه آنها یکی است
  - شناسائی با روش های signature based خیلی سخت است
- کرم های دگردیس(metamorphic)
  - هم شکل کد و هم عملکرد آن تغییر می یابد
  - استفاده از رمزنگاری برای مخفی کردن عملکرد

مشخصه های کرم ها



کرم های معروف در اینترنت

- IBM Christmas Card Virus، دسامبر ۱۹۸۷
- Morris Internet Worm، نوامبر ۱۹۸۸
- Code Red I, II
- Nimda
- Slammer
- Sasser
- Witty

Christmas Card Virus

- سیستم های EARN، BITNET و VNET را آلوده کرد.
- یک script ازطرق ممکن مانند email به کاربر منتقل می شود.
- با نشان دادن تصویر زیر، کاربران را ترغیب به دیدن اجرای فایل می کند
- شکل روبرو نشان داده شده و کاربر تشویق می شود

تا برنامه را اجرا کند

- با استفاده از دسترسی به فایل های mail alias و

بعضی از فایل های log خود را به کاربران دیگر ارسال می کند

Christmas Card Virus

- کرم با دسترسی به فایل های کامپیوتر آلود قربانی های بعدی را پیدا می کند
- کرم از نوع self-carried است.
- بوسیله کاربر و با استفاده از مهندسی اجتمای خود را اجرا می کند

Morris (Nov. ۱۹۸۸)

- بیشتر کرم های موجود از این کرم تقلید کرده اند.
- بدون کمک مهاجم و با سوء استفاده از آسیب پذیری ها تکثیر می شود.
- دارای بردارهای حمله (Attack Vector) مختلفی است.
- معماری های مختلفی را پشتیبانی می کند.

  Sun –

  Vax –

بردارهای حمله

- Backdoor در Sendmail
- Buffer Overflow در Fingerd
- حدس زدن پسورد
- Pre-authenticated Login از طریق rsh

خصوصیات

- الگوی انتشار
  - کامپیوترهای قربانی را از منابع مختلفی پیدا می کند.
    - ماشین هایی که در فایل forward. لیست شده اند.
    - تولید تصادفی آدرس ها
- پنهانسازی
  - استفاده از نام sh
  - به طور متوالی خود را fork می کند تا شماره پروسس تغییر کند.
  - استفاده از رمزنگاری

کرم های جدید

- خیلی شبیه کرم های کلاسیک هستند.
- کرم هایی که از طریق ایمیل انتقال می یابند، از جملات گول زننده در subject استفاده می کنند.
  - جایزه یک میلیون دلاری
  - دستگیری اسامه بن لادن با یک ویدئو در پیوست
- می توانند از خیلی از فایروال ها عبور کنند.

پنهانکاری

- استفاده از نام های فریبنده برای فایل های پیوست شده
- استفاده از یک پسوند قلابی: saddam_capture.jpg.exe
- پنهان شدن در فایل zip
- پنهان شدن در فایل zip رمزنگاری شده با پسورد
- تکنیک های زیادی برای پنهان شدن در هاست
  - استفاده از فایل های با نام عجیب

انتشار از طریق آسیب پذیری ها

- سوء استفاده از آسیب پذیری های ویندوز
- می توانند خیلی سریعتر تکثیر شوند.
- کرم slammer در مدت ۱۵ دقیقه اکثر اینترنت را پر کرد.

Code Red I

- نسخه اولیه آن در ۱۳ ژولای ۲۰۰۱ پدیدار شد.
- از آسیب پذیری سرور وب IIS استفاده می کند.
- ضعف
  - الگوریتم تولید عدد تصادفی آن از seed یکسان استفاده می کنند.
  - همه کپی های کرم به رشته ای از هاست های یکسان حمله می کنند.
- انتشار خطی
  - هاست های زیادی را آلوده نکرد.

Code Red I v2

- در ۱۹ ژولای ۲۰۰۱ پدیدار شد.
- الگوریتم تولید عدد تصادفی آن تصحیح شد.
- ماژول DDoS آن سایت www.whitehouse.gov را تحت حمله قرار داد.
- از طریق TCP منتقل می شود.
- Self-carried هستند.
- بعد از حمله، این کرم کاملاً از بین رفت.

Code Red II

- در ۴ آگوست ۲۰۰۱ پدیدار شد.
- در payload آن یک backdoor برای دسترسی نامحدود از راه دور
- ضعف
  - در ویندوزهای NT دچار مشکل می شد ولی روی ویندوز ۲۰۰۰ به خوبی کار می کرد.
- از تکنیک اسکن کردن محلی استفاده می کرد.

اسکن کردن محلی

- تلاش می کرد تا هاست هایی که نزدیک به آن هستند، آلوده شوند:
  - با احتمال ۳/۸ یک IP تصادفی از کلاس B انتخاب می کند.
  - با احتمال ۴/۸ یک IP تصادفی از کلاس A انتخاب می کند.
  - با احتمال ۱/۸ یک IP تصادفی از کل اینترنت انتخاب می کند.
- هاست های محلی اغلب شبیه هستند و انتشار سریعتر صورت می گیرد.

Nimda

- در ۱۸ سپتامبر ۲۰۰۱ پدیدار شد.
- انتشار Multi-mode:
  - حمله به سرور IIS از طریق کلاینت های آلوده
  - کپی کردن خود از طریق شبکه های مشترک
  - تغییر صفحات وب روی سرورهای آلوده برای آلوده کردن کلاینت ها
  - اسکن کردن برای پیدا کردن backdoorهای Code Red II و sadmind
- بعد از نفوذ از طریق IIS پورت ۸۰ با استفاده از TFTP کد را به سرور منتقل می کند.
- با نصب backdoor می تواند به عنوان zombie برای حملات DDOS استفاده شود.
- با کپی trojan hours در داخل باینری های موجود در web باعث می شود تا هرکسی به web وصل شود آلوده گردد.

Slammer Worm

- January 2003_
- کوچکترین کرم که دیده شده است.
- سوء استفاده از یک آسیب پذیری در MS SQL Server
- ارسال یک بسته UDP با حجم ۳۷۶ بایت به پورت ۱۴۳۴ سرریز بافر انجام می دهد.
- قربانی ها را با scan تصادفی پیدا می کند. (seed ها متفاوت)
- استفاده از UDP به جای TCP باعث افزایش سرعت انتشار می شود.
- فقط باعث کاهش کارائی کامپیوتر می شود.

Sasser

- April 2004
- هدف windows 2000 ,XP
- نفوذ از طریق سرریز بافر به روی سرویس Loacal Secuirty Authority Subsaytem برای دسترسی از راه دور و تکثیر
- استفاده از لینک مجزا TCP برای انتشار(Second Channel)
- استفاده از random scan
- بعد از نفوذ در قربانی، با استفاده ازFTP کد خود را از کامپیوتر قبلی می گیرد.
- قرار دادن یک کپی در دایرکتوری windows و اضافه کردن به رجیستری

کرم Witty

- March 2004
- از طریق نفوذ بر روی سرویسهای فایروال ISS : Real Secure sensor، BlackICEو...
- Self-carried
- تک ریختی
  - یک متن به شکل "^.^ insert witty message here ^.^" در داخل کد های خود دارد.
- ارسال بسته UDP به ۲۰۰۰۰ IP تصادفی با شماره پورت مبدا ۴۰۰۰
- در ماشین تصادفی به صورت تصادفی داده در دیسک می نویسد.
- توزیع توسط botnet

خلاصه کرم های معرفی شده

	Target finding scheme	Propagation scheme	Transmission scheme	Payload format
Morris	Blind	Self-carried	TCP	Monomorphic
Code Red	Blind*	Self-carried	TCP	Monomorphic
Nimda	Blind	Self-carried	TCP and UDP	Monomorphic
Slammer	Blind	Self-carried	UDP	Monomorphic
Sasser	Blind	Second channel	TCP	Monomorphic
Witty	Blind	Botnet	UDP	Monomorphic

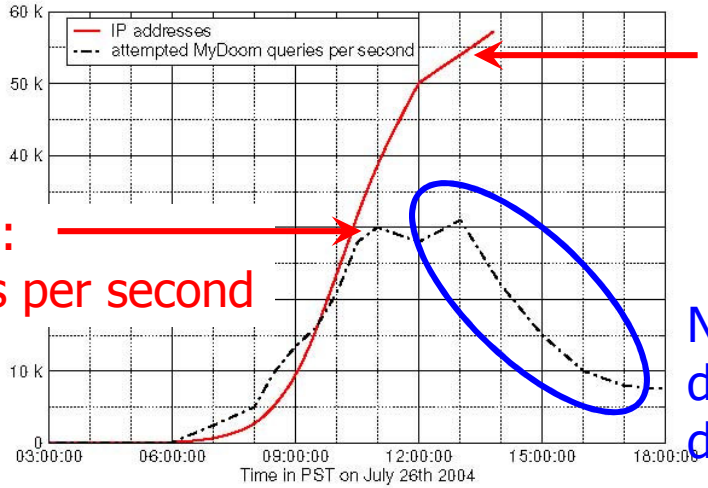
*Code Red II focuses on local subnet scan

MyDoom

- تکثیر با email
- MyDoom: هارد دیسک محلی را برای email های جدید می گردد.
- MyDoom.O: از سرویس موتور های جستجو مانند گوگل استفاده می کند.
- میزان در خواست ها بین متور های جستجوی مختلف:

Google (45%), Lycos (22.5%), Yahoo (20%) and Altavista (12.5%)

Google's view of MyDoom



Peak scan rate:
30,000 queries per second

Number of IP addresses generating queries (60,000 hosts infected in 8 hours)

Number of served queries drops as Google's anomaly detection kicks in

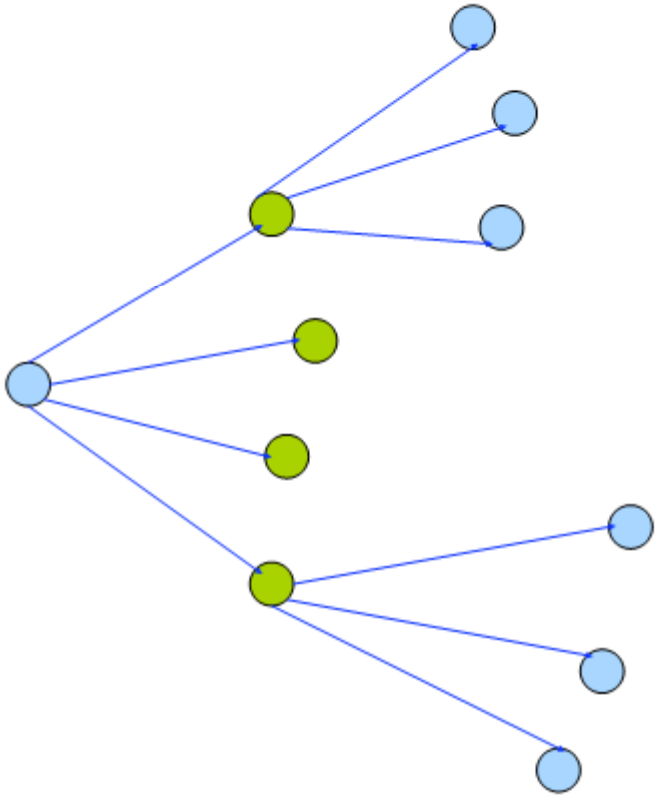
کرم های بهتر

- همه کرم ها دارای الگوی ارتباطی منحصر به فردی هستند.
- این باعث شناسایی خودکار کرم ها می شود.
- چگونه می توان این ضعف را برطرف کرد.

Contagion Worm

- فرض کنیم دو آسیب پذیری داریم:
  - Es: آسیب پذیری وب سرور
  - Ec: آسیب پذیری کلاینت
- کرم سرور (کلاینت) را با Es (Ec) آلوده می کند.
- سپس صبر می کند:
  - وقتی یک کلاینت آسیب پذیر رسید، آن را آلوده می کند.
  - وقتی سیستم به یک سرور آسیب پذیر وصل شد، آن را آلوده می کند.

Contagion Worm



Contagion Worm

- در سیستم های P2P خیلی خطرناک است:
  - فقط یک آسیب پذیری لازم است.
  - peerها نرم افزارهای یکسانی را اجرا می کنند.
  - اغلب فایل های بزرگ انتقال داده می شوند.

روش های شناسائی کرم ها

- شناسائی بر اساس امضا
  - امضا از قبل معلوم است
  - در NIDS قابل شناسائی است

روش های شناسائی کرم ها

- شناسائی بر اساس رفتا غیر نرمال
  - مناسب برای کرم های نا شناخته
  - بر اساس رفتار غیر نرمال ارتباطات: به عنوان مثال تعاد ارتباط tcp نا موفق(Connection Fail ratio)، تعداد پورت های بسته، اسکن کور و...
  - باتوجه به اسکن کور شناسائی بسته ها به طرف آدرس های استفاده نشده(darknet)
  - بر اساس ترافیک غیر مجاز
  - با استفاده از honeypot
  - براساس ساختار payload