



پژوهشگاه علوم و فناوری اطلاعات ایران



حملات منع سرویس، انواع، ابزارها و روند پیشرفت

نوید باباخانی

۱۳۹۴/۰۶/۰۹



DoS/DDoS
Concepts

DoS/DDoS
Attack
Techniques

DoS/DDoS
Attack
Tools

- معرفی حمله منع سرویس
- انواع حملات منع سرویس کلاسیک
- معرفی نوع توزیع شده منع سرویس
- انواع حملات منع سرویس توزیع شده
- ابزارهای موجود در اجرای حملات منع سرویس
- روند پیشرفت حملات منع سرویس
- جمع‌بندی

معرفی حمله منع سرویس

Denial of Service (DoS)

عملی به قصد مختل کردن یا آسیب رساندن به دسترسی مجاز

کارکرد شبکه و سیستم

منابع

برنامه‌های کاربردی

قربانیان منع سرویس:

فراهم کنندگان سرویس‌های اینترنتی (ISP)

بانک‌ها، بنگاه‌های اقتصادی، سایت‌های تجارت الکترونیکی

مراکز داده و ...

انواع حملات منع سرویس کلاسیک

سوء استفاده از یک اشکال سیستم:

حمله Land

ارسال بسته‌ای به یک ماشین با آدرس مبدأ و مقصد آن ماشین

Teardrop

ارسال قطعه‌های دارای همپوشانی از یک بسته IP

Jolt2

ارسال متوالی بسته‌های قطعه قطعه شده بدون قطعه اول

Winnuke و Nuke

ارسال بسته فاقد محتوای صحیح به پورت ۱۳۹ ویندوز

حملات سیل آسای پروتکل ICMP

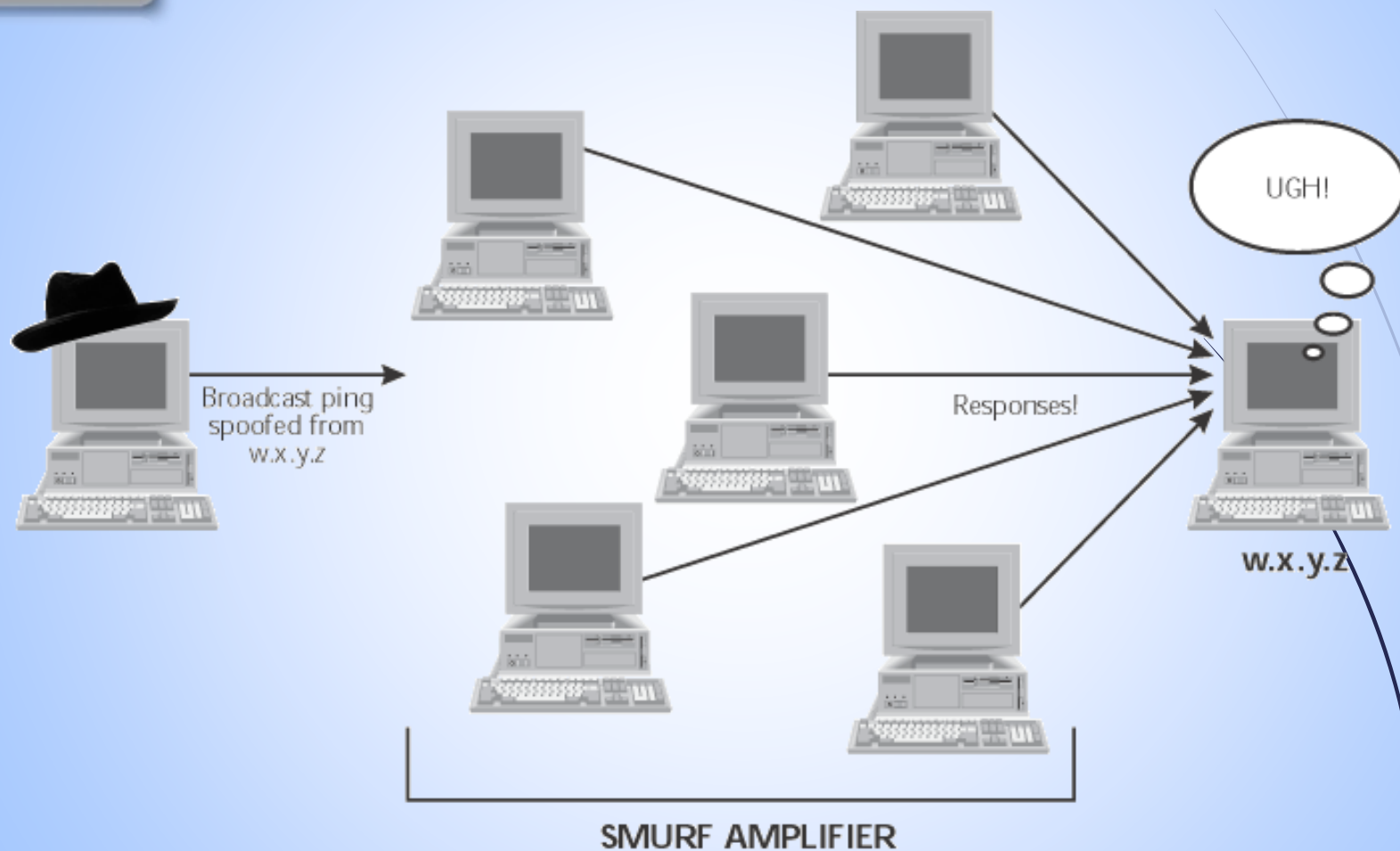
ارسال بسته ping با اندازه
بزرگتر از ۶۴ کیلوبایت

Ping of Death

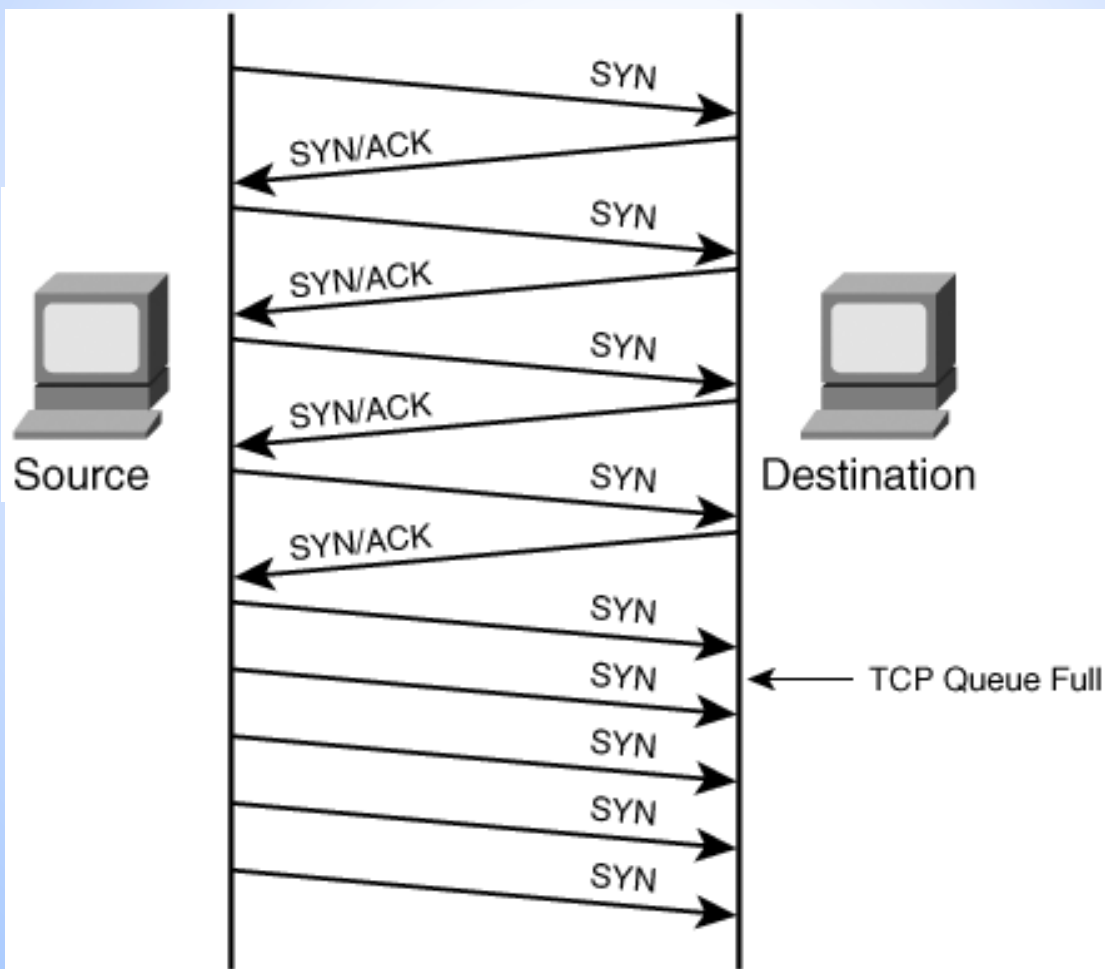
ارسال بسته ping بصورت
پی در پی و بدون وقفه

Ping Flood

Smurf



حمله سیل آسای TCP Syn



مثالی از Syn Flood سستی

MS Blaster worm (2003)

در ظهر ۱۶ آگوست سیستم‌ها آلوده شدند

حمله سیل SYN به پورت ۸۰ سایت **windowsupdate.com**

با شدت ۵۰ بسته SYN در هر ثانیه

هر بسته با طول ۴۰ بایت

آدرس IP جعل شده مبدأ: a.b.X.Y که X و Y تصادفی هستند

SSL/TLS handshake

سرعت رمزنگاری در RSA حدوداً ۱۰ برابر سرعت رمزگشایی

حمله HTTP POST DoS

ارسال درخواست HTTP با نرخ بسیار پایین

حمله RUDY (R-U-Dead-Yet?)

تداوم بخشیدن به نشست‌های HTTP با ارسال سرایندهای حجیم

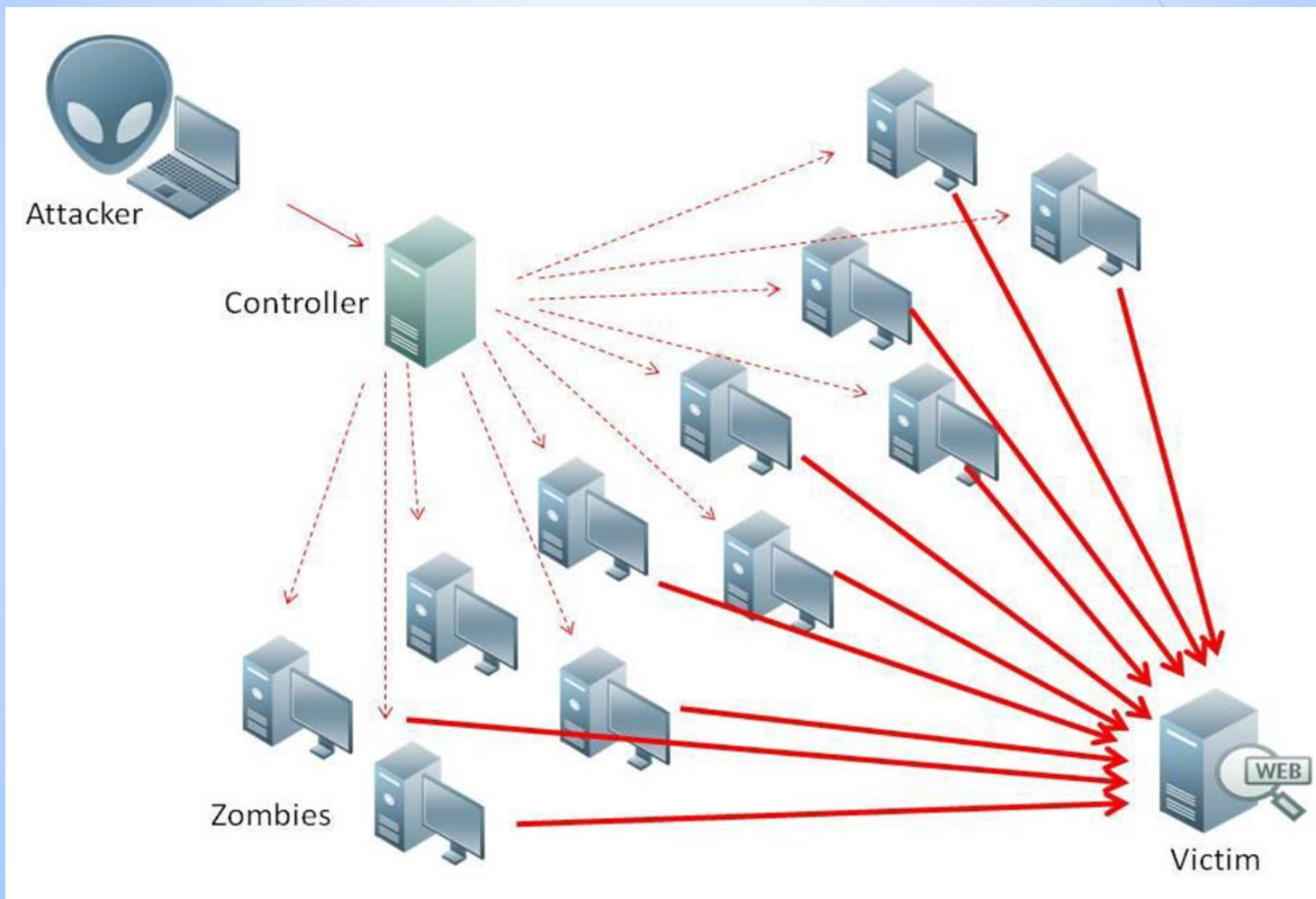
حملات منع سرویس توزیع شده

- استفاده از چندین سیستم برای حمله به یک سیستم

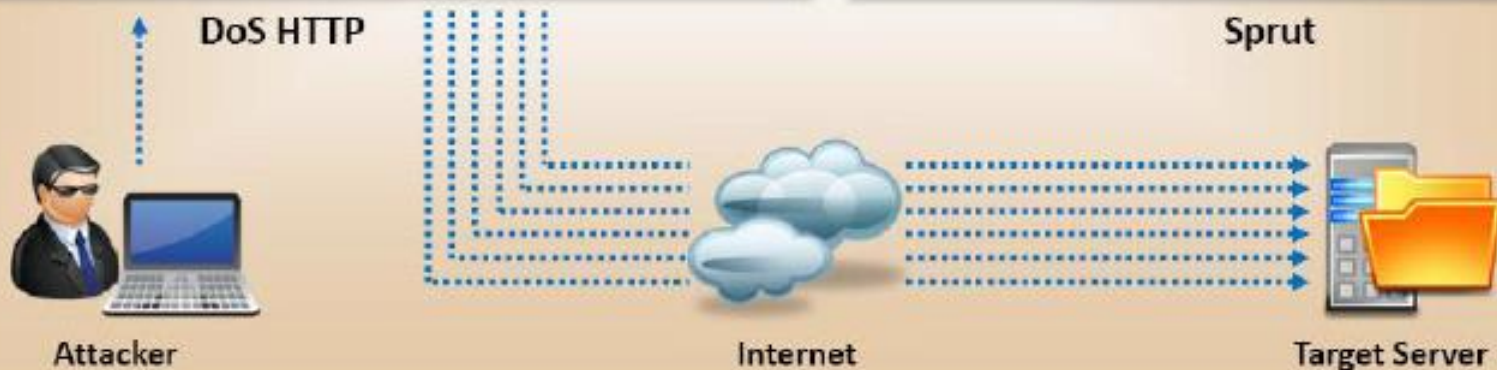
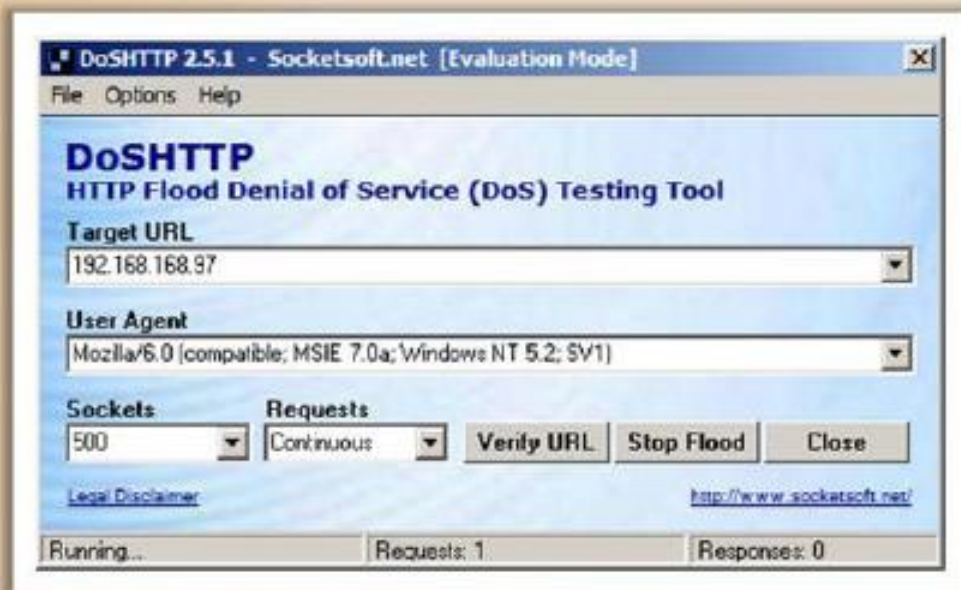
- ۲۰۰۰ eBay، Yahoo! و Amazon در فوریه

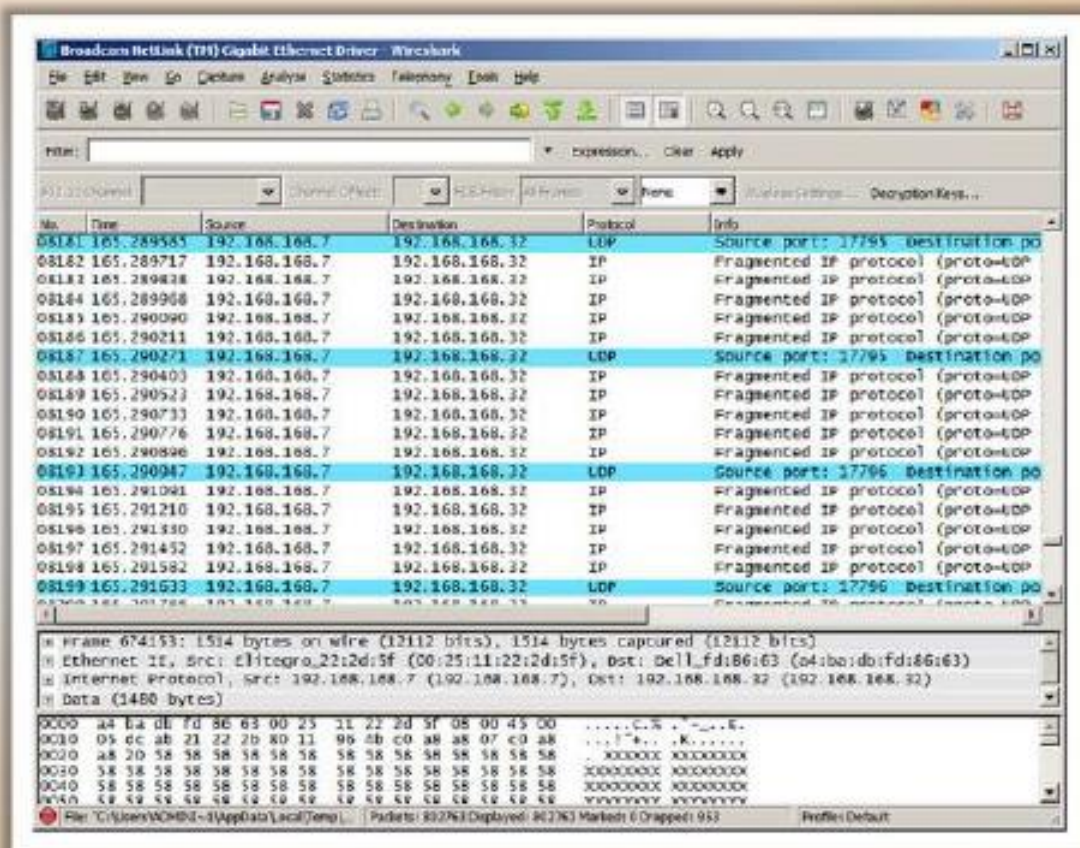
- یکی از رایج ترین حملات در اینترنت

- اغلب گزارش نشده اند



Volume Based	Protocol Based	Application Layer
پهنای باند مفید سرور را به شدت کاهش می‌دهد	مستقیماً منابع خود سرور را مصرف می‌کند	استفاده از آسیب‌پذیری نرم افزار در سطح لایه کاربرد برای از کار انداختن سرور
واحد: بیت در ثانیه	واحد: بسته در ثانیه	واحد: تقاضا در ثانیه
TCP flood UDP flood ICMP flood مثال:	Ping flood Smurf SYN flood مثال:	Hash DoS Teardrop مثال:





PHP DoS

Traffic at Victim Machine

```
[root@mandrake bin]#  
[root@mandrake bin]# gcc -o jolt2 jolt2.c  
[root@mandrake bin]# arp -s 10.10.0.254 00:11:22:33:44:55  
[root@mandrake bin]# ./jolt2 10.10.0.254  
  
[root@mandrake bin]#
```

Jolt2

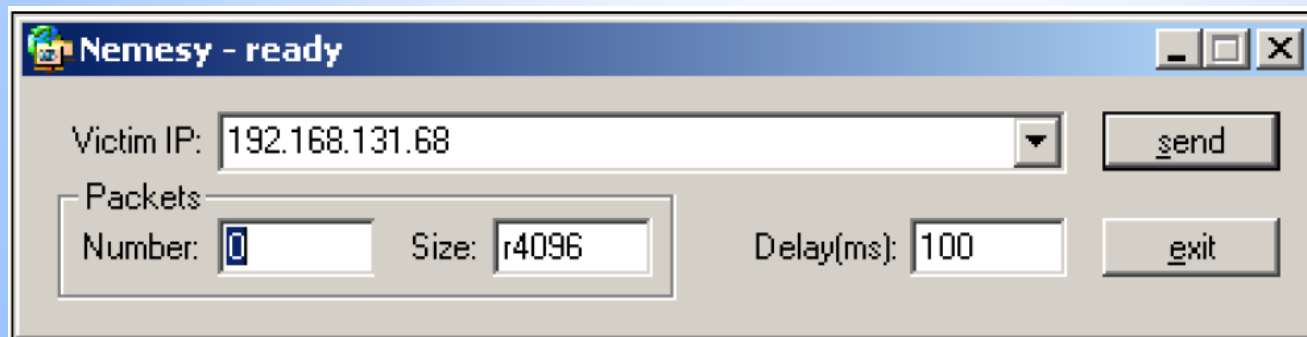
Bubonic.c

Land & LaTierra

Nemesy

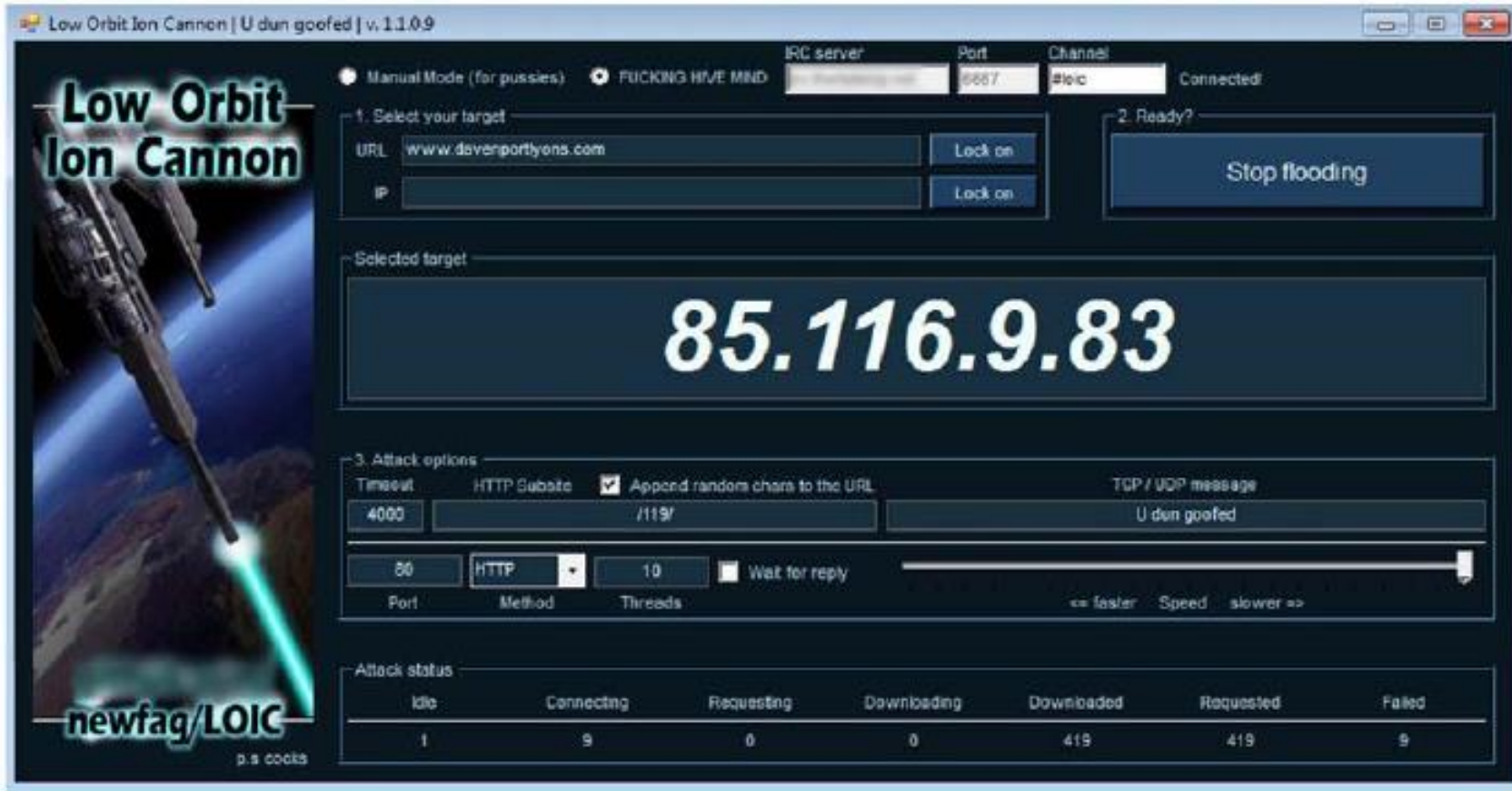
Crazy Pinger

UDP Flood



- Tribe Flood Network
- TFN2K
- Blitznet
- MStream
- Trin00
- Trinity
- Shaft
- Stacheldraht (“barbed wire”)
- LOIC

- ▶ جانشینی برای Tribe Flood Network
- ▶ ایجاد شبکه‌ای از زامبی‌ها و اجرای حملاتی مانند:
 - ▶ UDP flood
 - ▶ SYN flood
 - ▶ ICMP flood
 - ▶ Smurf attack
 - ▶ “Mix” attack using UDP, SYN, and ICMP floods
- ▶ عدم تشخیص زامبی‌ها توسط ابزار Nmap
- ▶ جعل آدرس مبدأ توسط زامبی‌ها
- ▶ دشواری در یافتن مهاجم



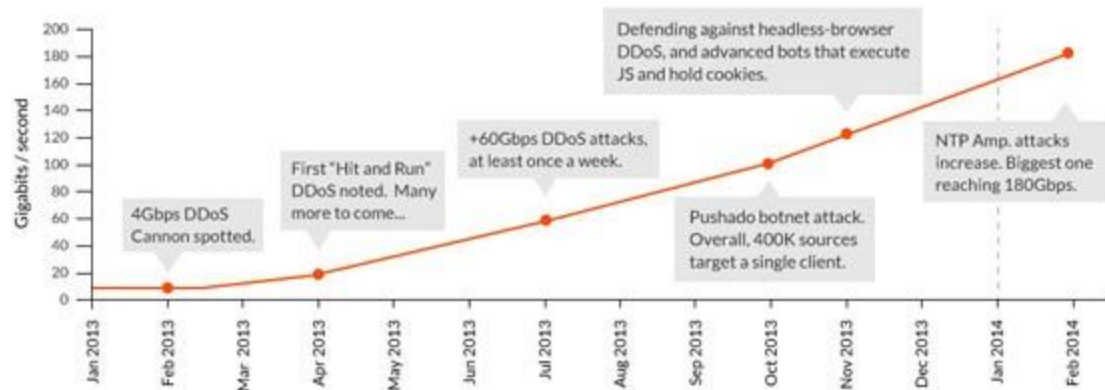


رند پیشرفت حملات منع سرویس

18/20

DDoS Attack Trends 2013-2014

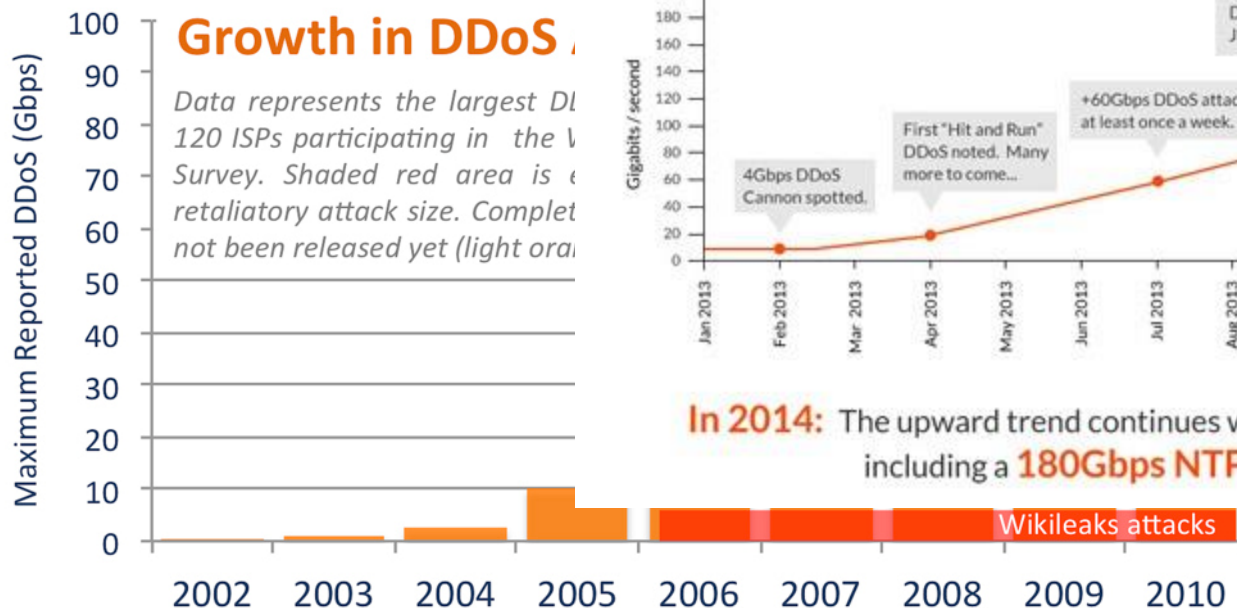
In 2013: Rapid increase in peak attack volumes and bot sophistication.



In 2014: The upward trend continues with several ~100Gbps threats, including a **180Gbps NTP DDOS attack**.

Growth in DDoS

Data represents the largest DDoS attack seen by 120 ISPs participating in the survey. Shaded red area is a retaliatory attack size. Complete data not been released yet (light orange).

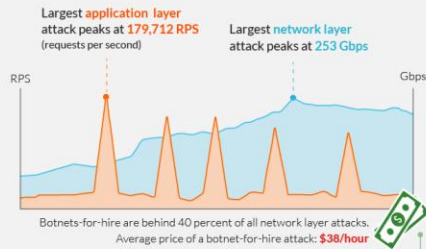


Q2 2015 Global DDoS Threat Landscape

Tenacious Attacks Resemble Advanced Persistent Threats

Analysis is based on data from 1,572 network layer and 2,714 application layer DDoS attacks mitigated by Incapsula services from March 1 through May 7, 2015.

Information about DDoS bot capabilities and assumed identities comes from a sample of 60 million DDoS bot sessions collected over the same period.



Frequency High and Duration Long



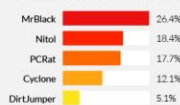
Every hour of unmitigated DDoS costs a business **\$40,000**. Persistent attacks entail losses of hundreds of thousands—if not millions.



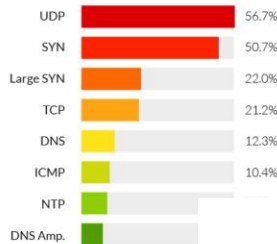
Botnets' Global Footprint

- 56 percent** of DDoS bot traffic emerged from **China, Vietnam, US, Brazil, and Thailand**.
- MrBlack** botnet is the **most aggressive**, despite not being the largest.

Most aggressive DDoS botnets



Network Layer Attack Trends

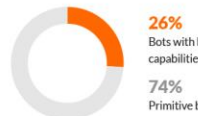


UDP is the most common attack method, used in **56 percent** of attacks.

Of these, eight percent are **SSDP** DDoS attacks, launched from "Internet of Things" devices.

- More than half** of all network attacks are **multi-vector**.
- DNS and NTP amplification** is out of favor.
- Large-SYN** floods cause the most damage.

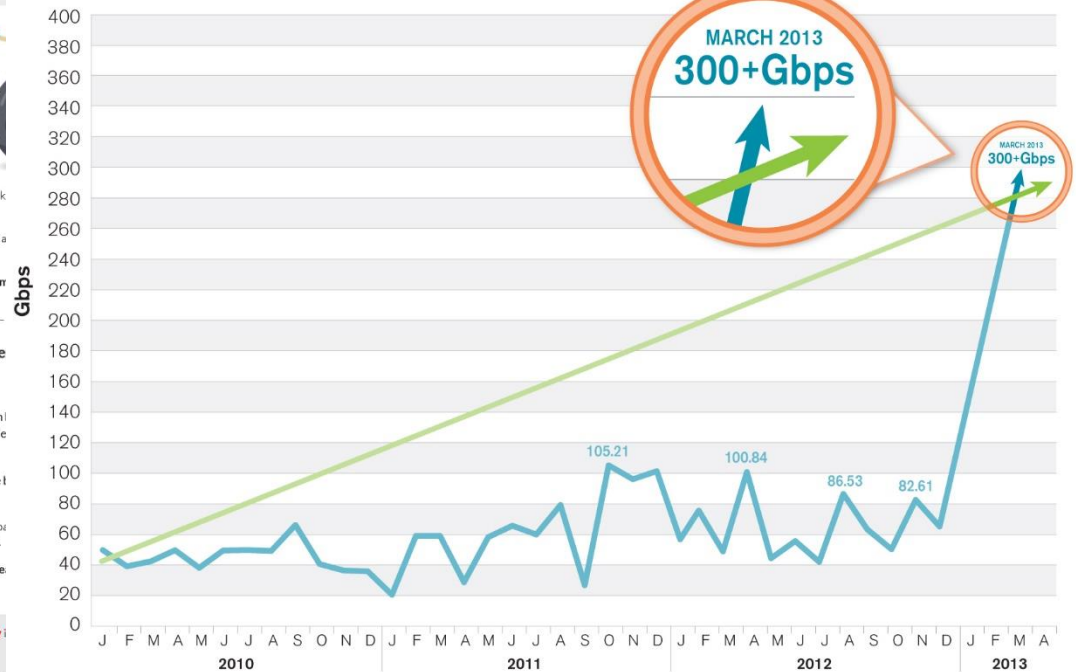
Application Layer Attack Trends



- DDoS bots mimic browser capabilities to **bypass security measures**.
- Steep drop in the number of **session impersonators**.

Analysis points to **higher diversity** in assumed identities.
Ten most common fabricated user-agents used in 43 percent of attacks (down percent in 2014).

Peak DDoS Attack Size (January 2010-Present)



Source: Arbor Networks, Inc.

19/20

DDoS Thugs Adopt APT-like Tactics

Offenders are mounting advanced attacks that resemble advanced persistent threats.

Targeted
Specific targets are chosen in advance. Attackers conduct early reconnaissance to expose targets' weaknesses.

Persistent
Attackers orchestrate complex multiphase and multi-vector assaults. Individual attacks can easily last for days, weeks, or even months at a time.

Advanced
Attackers coordinate DDoS assaults with other cyberattacks. Stealth tactics are employed to bypass security countermeasures.

پژوهشگاه علوم و فناوری

ARBOR
NETWORKS

حمله‌ات منع سرویس تهدید واقعی برای بسیاری کاربران اینترنت هستند.

پیش‌بینی حملات DDoS:

افزایش در اندازه

افزایش در پیچیدگی

افزایش حملات معنایی DDoS

حملات زیرساختی

حملات DDoS تهدید جدی برای پایداری و رشد آتی اینترنت هستند.

سوال و جواب

