ESTONIAN & GEORGIAN CYBER ATTACKS

Toomas Lepik

CERT Eesti
Computer Emergency Response Team

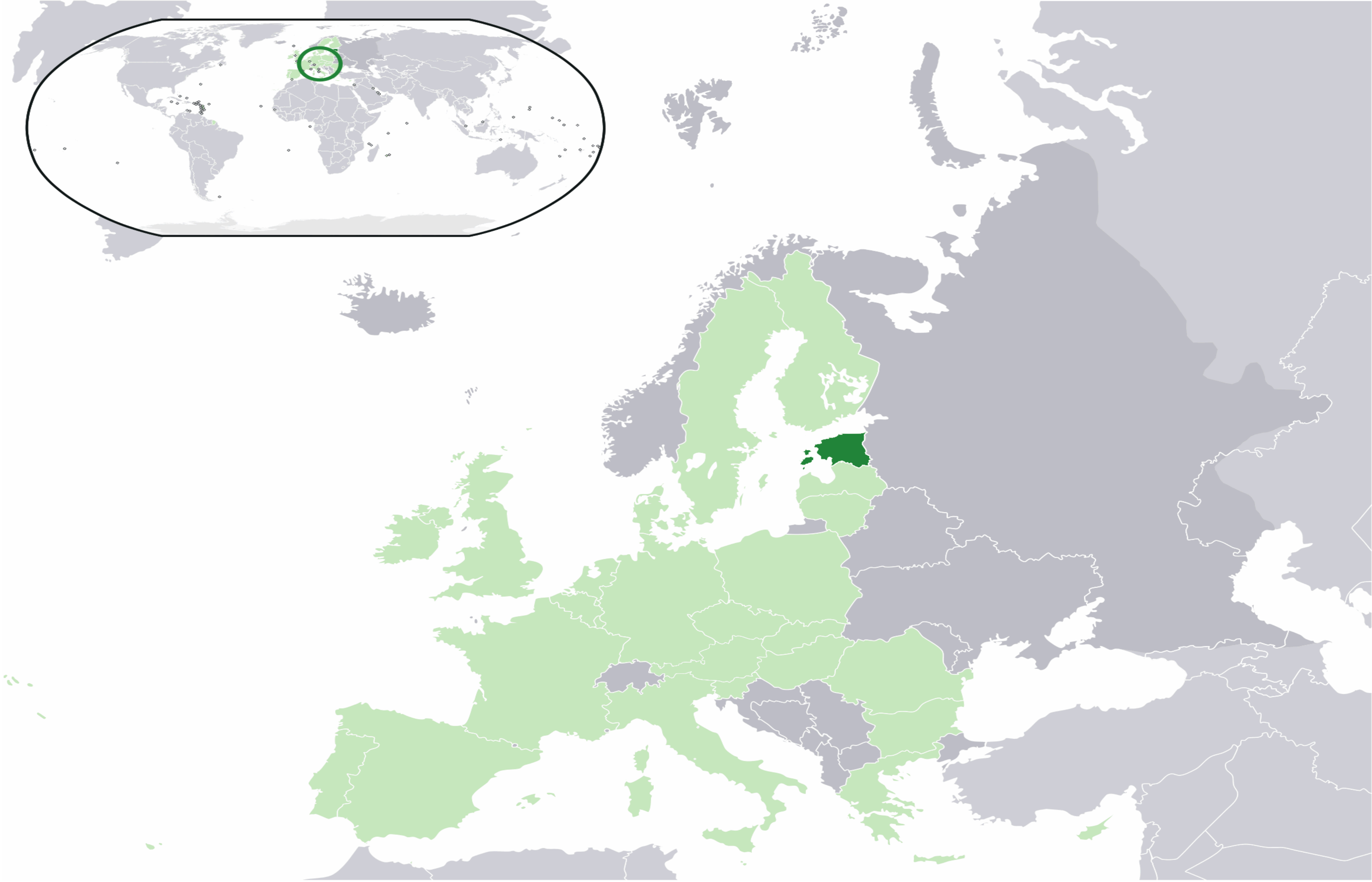
David Tabatadze

GRENA
Georgian Research and Educational Networking Association

21st Annual FIRST Conference
KYOTO June 28-July 3, 2009

- ✓ Quick recap - Estonian Story
- ✓ Georgian events
- ✓ Was there any commonalities
- ✓ How the incidents were handled
- ✓ What we can learn

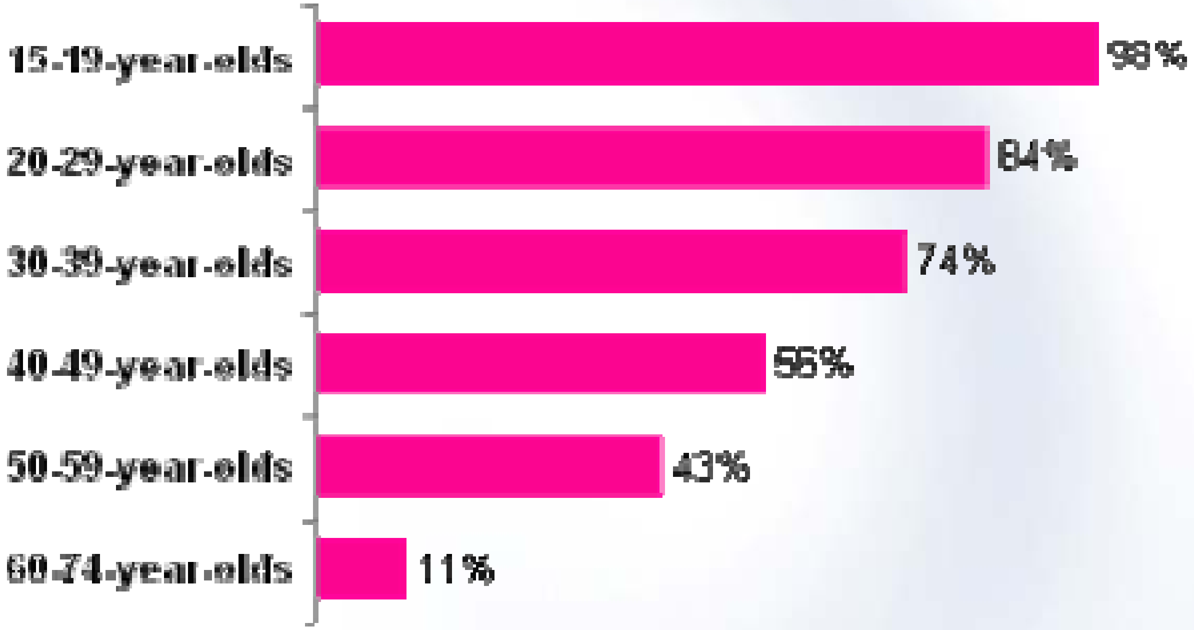
ESTONIA



ESTONIA

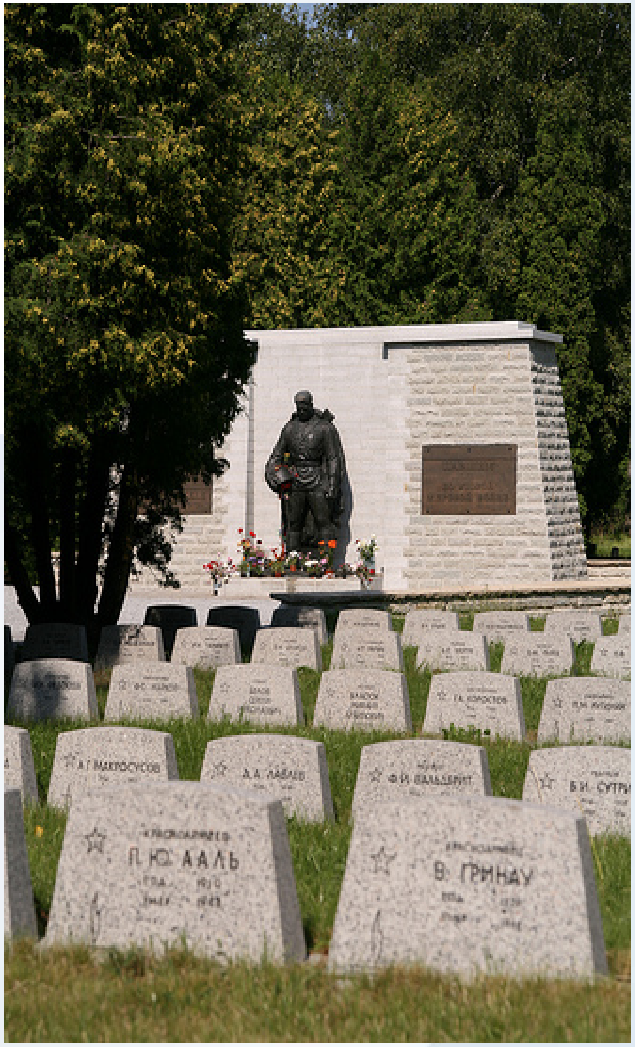
1st quarter of 2008 58% of Estonian households had access to the Internet at home

Internet usage in Estonia – in different age groups in 2006



Why It started sort story

Я ПОМНЮ!
Я ГОРЖУСЬ!
ДЕНЬ ПОБЕДЫ НАД ФАШИЗМОМ
9 МАЯ 1945 ГОДА



Time line of events in internet

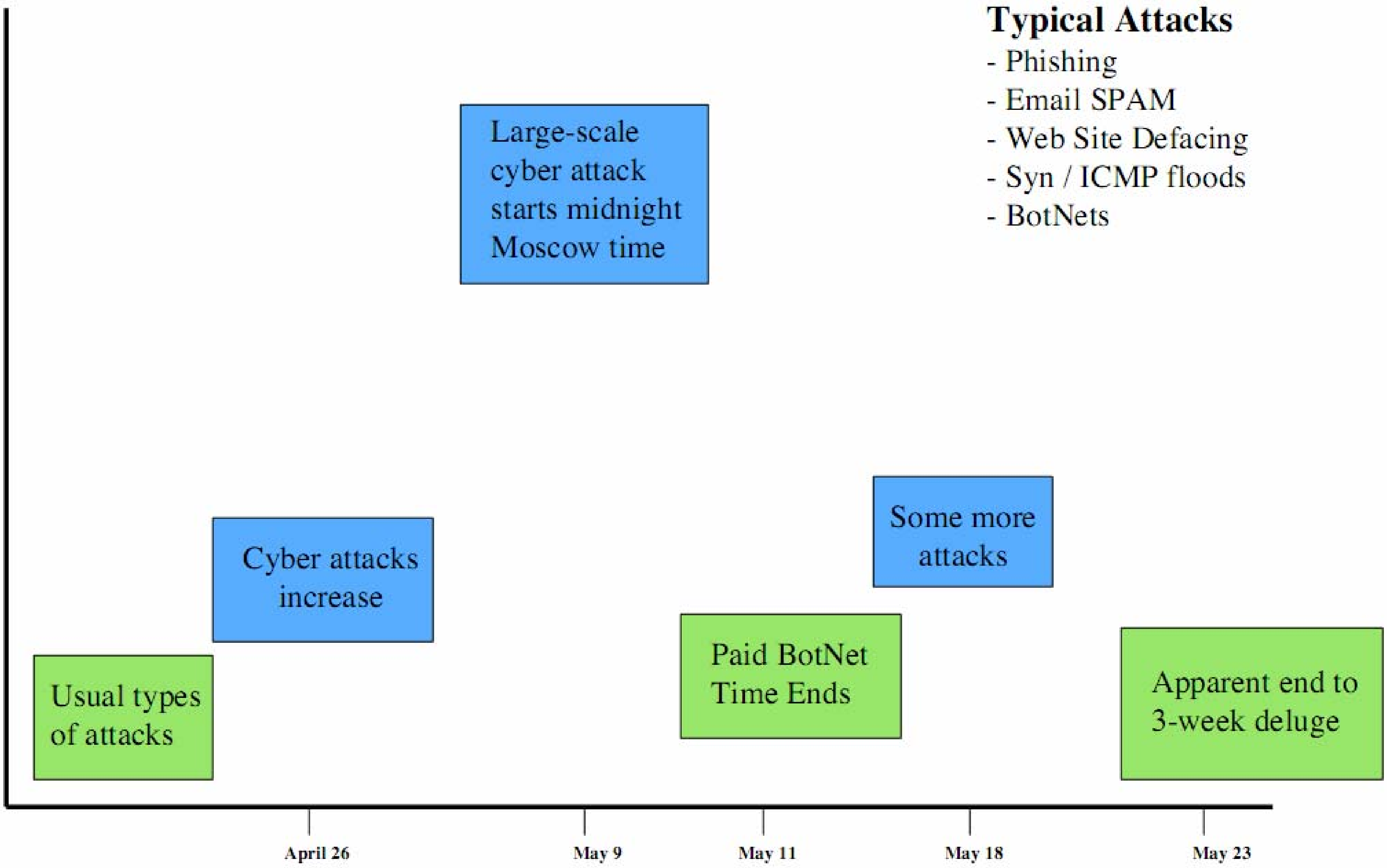
•Mid of april - first notes about attacks to be
•done on May 9

•Frst attack was launched on 27.04.07 22:30

•Saturday and Sunday (28.-29.04) - a number of small scale attacks on different target (gov, media) with different vectors and different impact (first ISP down)

•Поздравь с 9 Мая по E-mail
•May 9 - 08.05.07 23:00 new wave

Time line of Events



Typical Attacks

- Phishing
- Email SPAM
- Web Site Defacing
- Syn / ICMP floods
- BotNets

Usual types of attacks

Cyber attacks increase

Large-scale cyber attack starts midnight Moscow time

Paid BotNet Time Ends

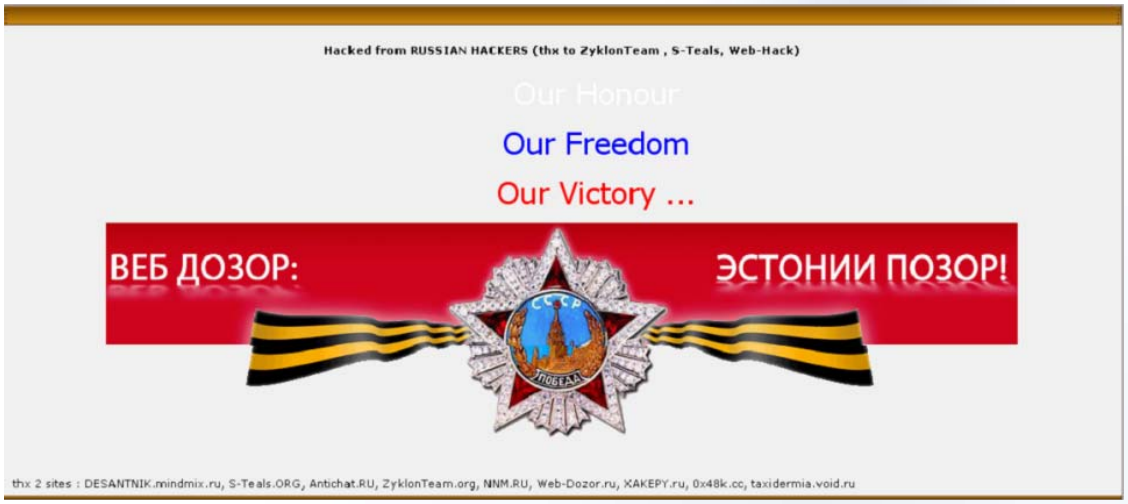
Some more attacks

Apparent end to 3-week deluge

(Note: Timeline not to scale)

What were done

Defacement's
Defacement's whit time bombing
SPAM DDos
DDos
Attacks on routers



Hacked from RUSSIAN HACKERS (thx to ZyklonTeam , S-Teals, Web-Hack)

Our Honour

Our Freedom

Our Victory ...

ВЕБ ДОЗОР: ЭСТОНИИ ПОЗОР!

thx 2 sites : DESANTNIK.mindmix.ru, S-Teals.ORG, Antichat.RU, ZyklonTeam.org, NNM.RU, Web-Dozor.ru, XAKEPY.ru, 0x48k.cc, taxidermia.void.ru

Who / What were involved

People ,botnets , computers

Estonian president had say to the matter.

The attacks on my irrelevant homepage [laughs] were not that bad. It was just knocked out. But for more serious things, first of all, the national emergency number, 112, was hit. That was mercifully out of commission for a very short time, but had there been at that time when it was briefly out of commission a fire, a heart attack, it would have been...someone could have died. It was a problem for banks because 97 percent of bank transactions in my country are over the Internet, which one of our main responses was to keep out all computer messages from outside the country code .ee, as you [here in the Czech Republic] have .cz. Here in Europe, we have country codes.

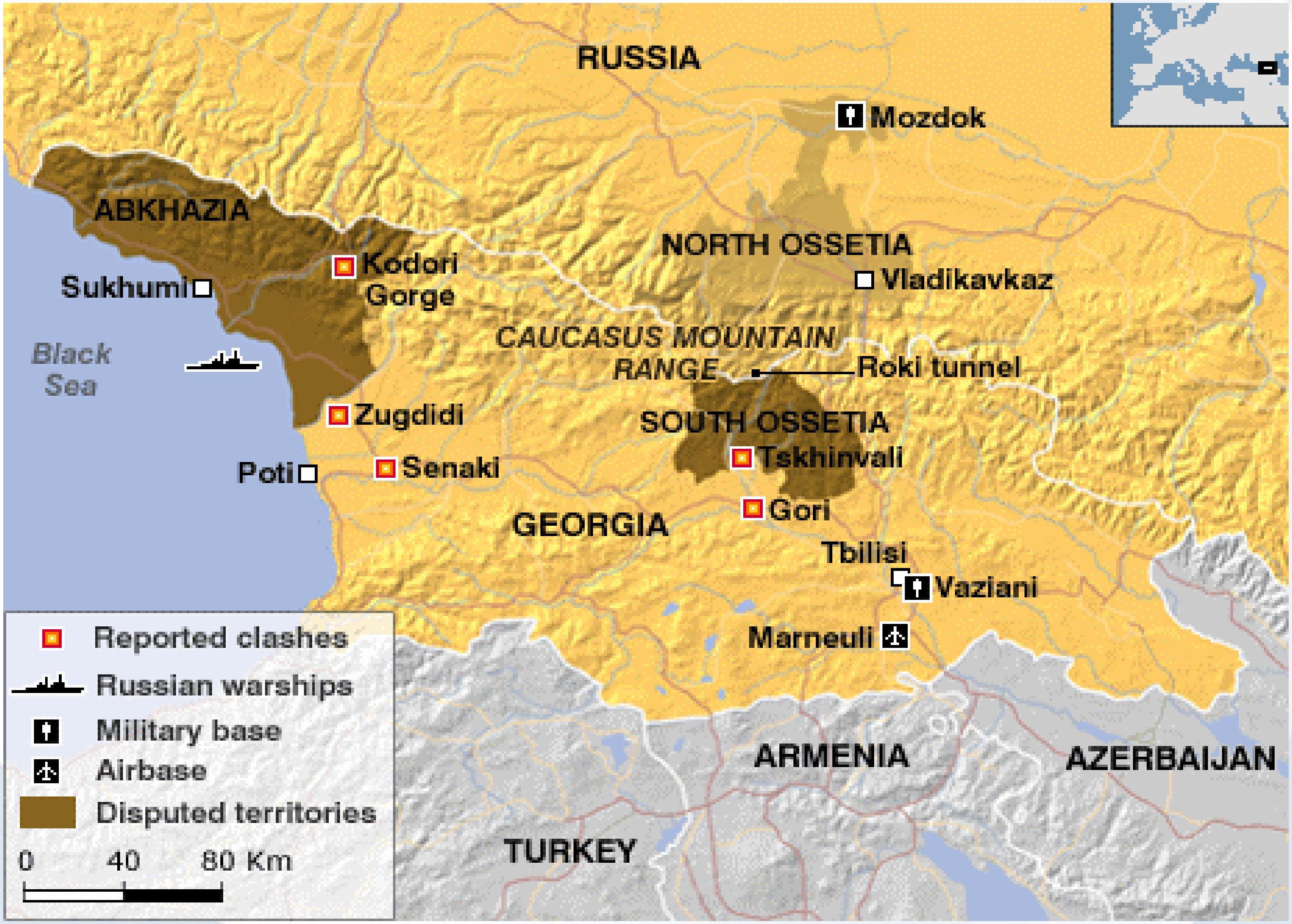
What that meant was that you could access pages inside the country, but you couldn't from the outside. So if you wanted to go into your bank account from outside then, of course.... Being a very open country with one of the highest trade-to-GDP ratios in the world, I think No. 2 after Hong Kong, that means it does affect you.

This presentation actually is about Georgia (not in United states)

Georgia

GE - 4,630,841 population - Area: 69,700 sq km

Capital city: Tbilisi - population 1,026,874



Timeline of events in physical world

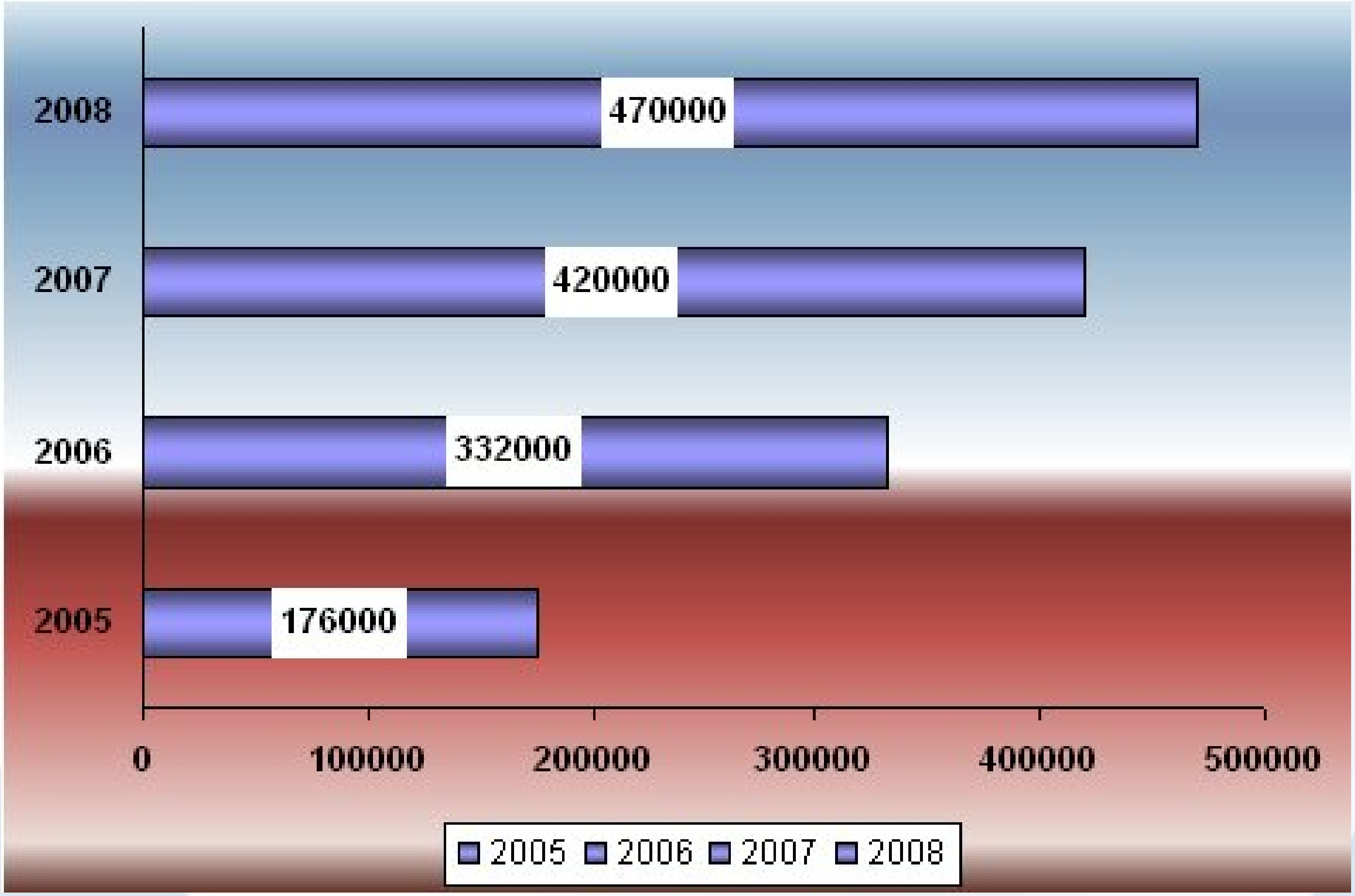
- 1-6 August - Georgian-controlled villages come under intense fire from the South Ossetian separatists, Georgian police respond by firing towards the separatist militia.
- 7 August - South Ossetian separatist government leader threatens to "clean Georgians out" from the region. The President of Georgia announces a unilateral cease fire and separatist government of South Ossetia refuses to negotiate with Georgian envoy. Separatist authorities open fire on all Georgian checkpoints around the South Ossetian capital. South Ossetian paramilitaries and Russian peacekeepers direct heavy fire on Georgian peacekeepers. 100 Russian armored vehicles and Russian troops invade Georgia, crossing the Roki Tunnel from Russia into Georgia
- 8 August - For the first time, and in response to the entry of Russian armed forces into Georgian sovereign territory, Georgian military enter the conflict zone. Part of Tskhinvali and some villages comes under the control of the Georgian army and fighting continues. The Georgian government announces a ceasefire from 15.00 till 18.00 to allow civilians to leave Tskhinvali. The Government of Georgia offers the separatists full amnesty and humanitarian aid if they surrender. Russia bombs Georgian airfields.
- 9 August - Russians bomb vital port of Poti, attacks railway station and military base in town of Senaki, bombs an airfield in the outskirts of Tbilisi and bombs several cities close to conflict zone.
- 10 August - Early morning 6,000 Russian troops enter Georgia through Roki tunnel: 90 tanks, 150 Armored Personnel Carriers, 250 artillery gunships.
- 11 August – Russian troops occupies several cities, destroy Georgian military bases, continue bombing strategic purposes

More information: http://aillarionov.livejournal.com/12380.html

Internet usage survey

- 470,000 Internet users as of Nov/08, 10.3 % penetration, per ITU.

- 48,700 broadband Internet connections as of Nov/08, 1.2 % penetration, per ITUper ITU.



How the attacks were discovered

- ❑ TBC Bank – Biggest bank in Georgia
- ❑ CERT-Polska – Poland
- ❑ Georgian Internet Service Providers

  - *United Telecom of Georgia*

  - *Caucasus Online*

It was reported that attacks started on August 9 but we discovered it on August 11

Why the attacks on internet mattered at all ?

Cyber attacks had far less impact on Georgia than they might on a more Internet-dependent county, like Estonia or the United States, where vital services like transportation, power and banking are tied to the Internet.
Although reasons were also very crucial in terms of war in the country:

- Misinformation of real facts by Russian Media
- Aggression and patriotic spirit of Russian supporters.
- Block and cut off Georgian Internet resources
- Shut down media , forums, blogs in Georgia.
- Impact on the Georgia's visibility on the internet and ability to communicate with the world.
- Make panic and as much damage as possible to the critical infrastructures.

Types of attacks beside physical

86.105.36.3	Romania,
87.4.147.122	Telecom Italia, Roma
220.215.92.36	FreeBit, Tokyo
194.250.18.253	France Telecom, Toulouse
92.49.146.212	VolgaTelecom, Orenburg, Russia
41.196.241.237	Link Egypt, Dokki-Giza
80.188.107.226	Telefonica O2 Czech Republic, Prague
83.37.61.226	Telefonica de Espana, Madrid
62.150.55.34	Qualitynet Co., Kuwait
80.224.161.231	Techauna AUNA, Barcelona
210.215.124.92	Nexon Asia Pacific, Sydney
75.101.230.118	Amazon Web Services, Seattle
217.209.224.115	Telia Network, Sweden
80.201.63.237	Belgacom ISP SA/NV, Bruxelles
212.92.140.142	Business Communication Agency, Russia
201.216.170.220	Telgua, Guatemala
88.168.106.155	Free SAS / ProXad, France
77.28.79.99	Makedonski Telekom, Skopje
194.29.60.35	Universal Telecom, Kiev, Ukraine

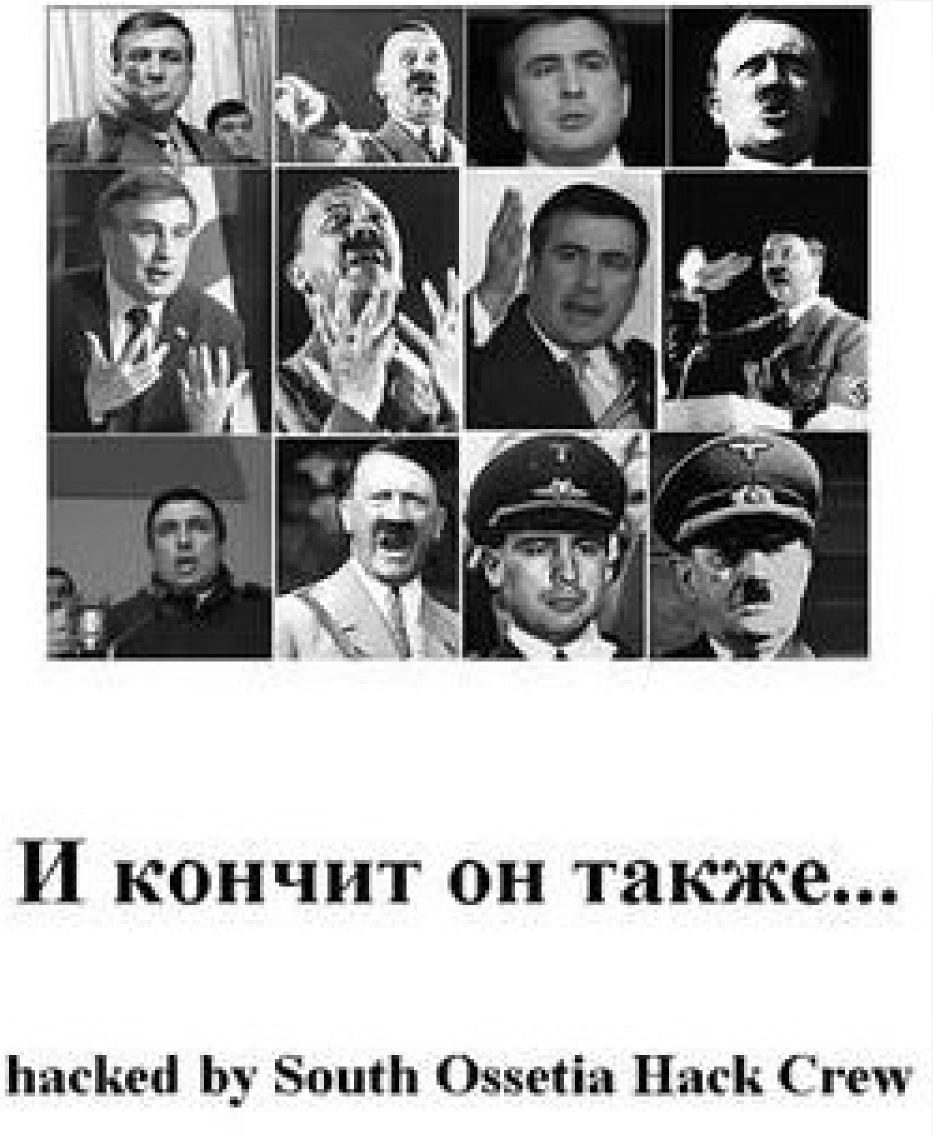
Types of attacks:

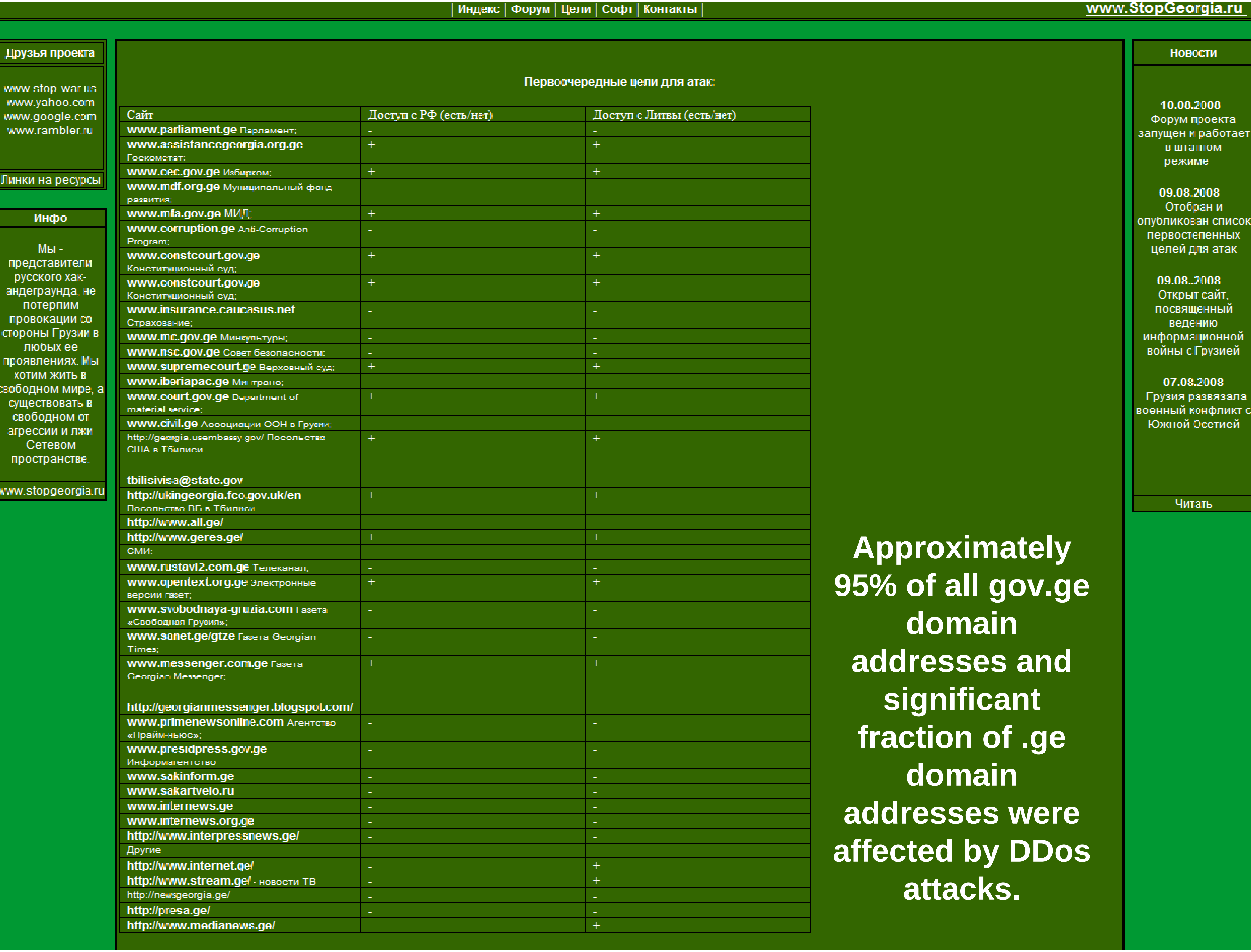
- SYN Flood
- Ping Flood
- Http Flood
- HACKING
- SPAM
- Port Scanning
- BOTNETS
- SQL Injections
- Malicious javascripts
- I-frames

Protocols:

- HTTP
- ICMP
- FTP
- SMTP
- DNS

What can be seen in internet





| Индекс | Форум | Цели | Софт | Контакты |

www.StopGeorgia.ru

Друзья проекта

www.stop-war.us
www.yahoo.com
www.google.com
www.rambler.ru

Линки на ресурсы

Инфо

Мы - представители русского хак-андеграунда, не потерпим провокации со стороны Грузии в любых ее проявлениях. Мы хотим жить в свободном мире, а существовать в свободном от агрессии и лжи Сетевом пространстве.

www.stopgeorgia.ru

Первоочередные цели для атак:

Сайт	Доступ с РФ (есть/нет)	Доступ с Литвы (есть/нет)
www.parliament.ge Парламент;	-	-
www.assistancegeorgia.org.ge Госкомстат;	+	+
www.cec.gov.ge Избирком;	+	+
www.mdf.org.ge Муниципальный фонд развития;	-	-
www.mfa.gov.ge МИД;	+	+
www.corruption.ge Anti-Corruption Program;	-	-
www.constcourt.gov.ge Конституционный суд;	+	+
www.constcourt.gov.ge Конституционный суд;	+	+
www.insurance.caucasus.net Страхование;	-	-
www.mc.gov.ge Минкультуры;	-	-
www.nsc.gov.ge Совет безопасности;	-	-
www.supremecourt.ge Верховный суд;	+	+
www.iberiapac.ge Минтранс;		
www.court.gov.ge Department of material service;	+	+
www.civil.ge Ассоциации ООН в Грузии;	-	-
http://georgia.usembassy.gov/ Посольство США в Тбилиси **tbilisivisa@state.gov**	+	+
http://ukingeorgia.fco.gov.uk/en Посольство ВБ в Тбилиси	+	+
http://www.all.ge/	-	-
http://www.geres.ge/	+	+
СМИ:		
www.rustavi2.com.ge Телеканал;	-	-
www.opentext.org.ge Электронные версии газет;	+	+
www.svobodnaya-gruzia.com Газета «Свободная Грузия»;	-	-
www.sanet.ge/gtze Газета Georgian Times;	-	-
www.messenger.com.ge Газета Georgian Messenger; **http://georgianmessenger.blogspot.com/**	+	+
www.primenewsonline.com Агентство «Прайм-ньюс»;	-	-
www.presidpress.gov.ge Информагентство	-	-
www.sakinform.ge	-	-
www.sakartvelo.ru	-	-
www.internews.ge	-	-
www.internews.org.ge	-	-
http://www.interpressnews.ge/	-	-
Другие		
http://www.internet.ge/	-	+
http://www.stream.ge/ - новости ТВ	-	+
http://newsgeorgia.ge/	-	-
http://presa.ge/	-	-
http://www.medianews.ge/	-	+

Новости

10.08.2008
Форум проекта запущен и работает в штатном режиме

09.08.2008
Отобран и опубликован список первостепенных целей для атак

09.08..2008
Открыт сайт, посвященный ведению информационной войны с Грузией

07.08.2008
Грузия развязала военный конфликт с Южной Осетией

Читать

Approximately 95% of all gov.ge domain addresses and significant fraction of .ge domain addresses were affected by DDos attacks.

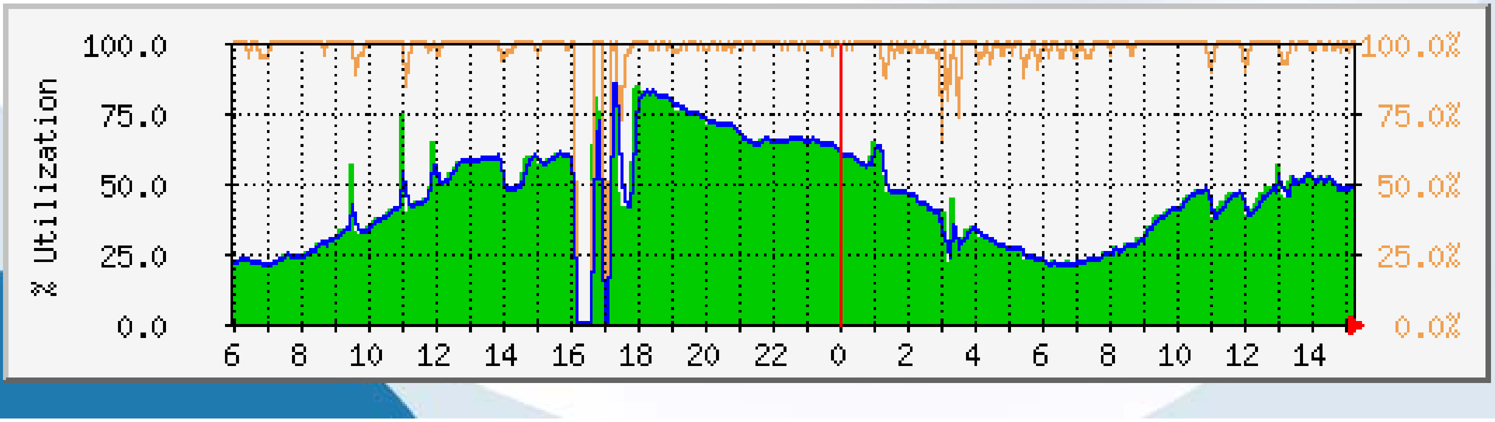
Internet Service Provider’s Problems

- Situation was also sharpened by fact that Georgian ISP’s had not enough internet bandwith capacity and because eof this attacks overloaded all channels and internet became too slow.

- Starting 9 August permanent attacks were handled to Georgian ISP’s border routers.
  There were following cases: Border Gateway Router’s CPU loaded 100%, even it was not able to control from console connection, it was shown in “*show proc cpu*” that IP INPUT and BGP Processes loaded processor. Meantime layer 3 switches at Border gateway were not affected by attacks and only Cisco 7206 Routers were overloaded. There was no entries in the logs files and the cause of overload.

- ISP’s System/Network Administrators had few experience with such massive attacks and also no CERT activity. Weak co-operation between ISP’s, hosting providers and actual owners of the websites.

Example: *United Telecom of Georgia Cisco 7206 CPU Statistics per day*

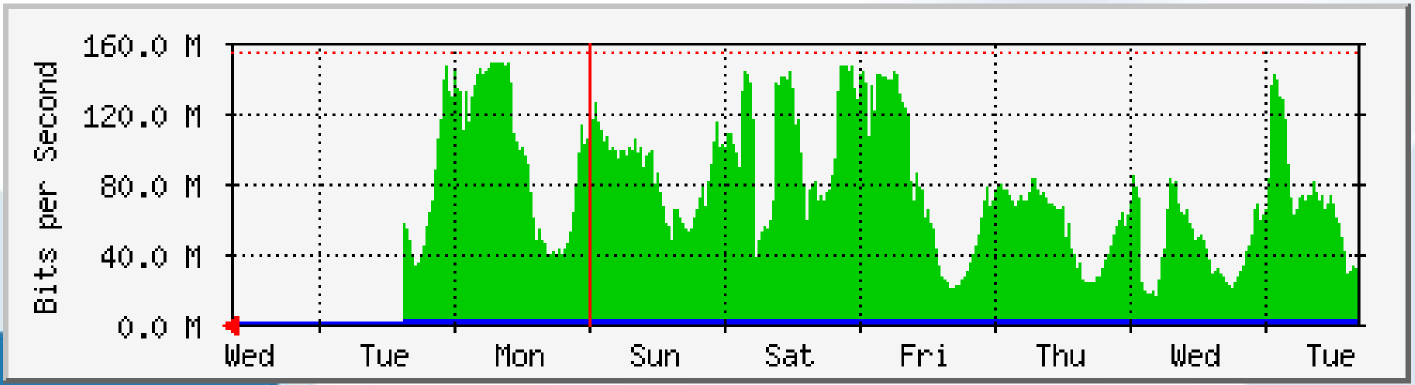


What we know about how it was done

“Power to the people”

- ❑ Russian Hackers web sites (StopGeorgia.ru and Xakep.ru) spreaded all necessary information and tools how to attack Georgian web-sites
- ❑ Target web sites and codes for attacks were posted in comments of hundred forums, blogs, news and entertainment web-sites
- ❑ Interested individuals were asking others to help and to join in by continually sending ICMP traffic via the 'ping' and explaining how to do it.
- ❑ At the same time ready bat files designed to attack Georgian websites detailed list of websites attack Georgian websites were spreaded using file exchange programs.

Example: Interpressnews.ge (News agency) –
detected traffic of about 150 MB. Site was periodically going down or working too slow



What we know about how it was done

“Hackers tricks”

- ❑ **Geographically distributed BOTNETS**

  * 300-400 sessions per IP per server

- ❑ **SQL INJECTION of more than 100 sites**

  *Examples:http://www.president.gov.ge/index.php?l=G&m=0&sm=3&id=2693+union+select+1,2,3,4,5,6,7,8,9,0,1,2,3,4,5
  http://www.results.cec.gov.ge/ubnebi.php?district=22+and+1=@@version
  http://junior.eurovision-georgia.ge/index.php?lang=eng&topid=3&id=-1+union+select+1,2,3,4,5

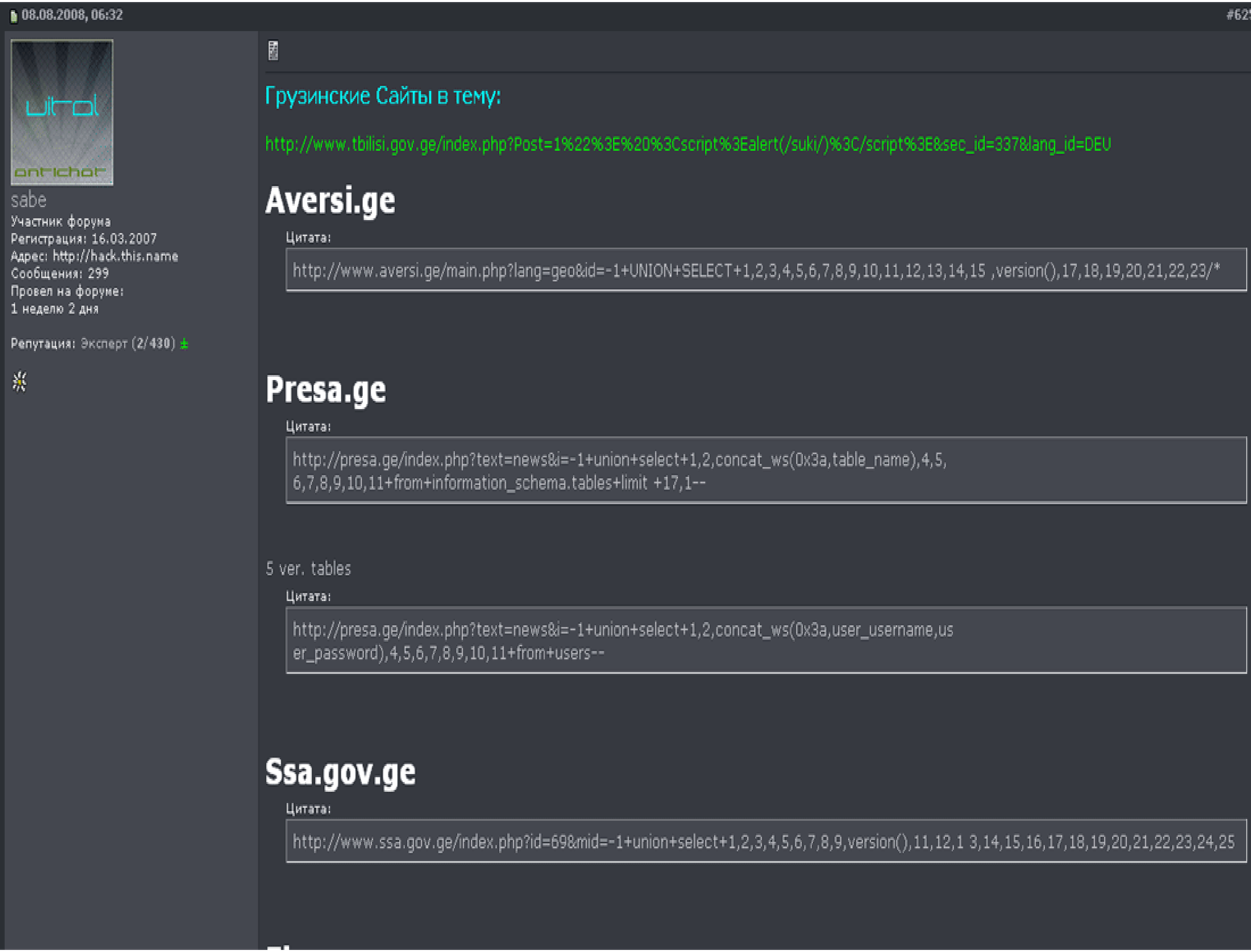
- ❑ **Attempts of BGP hijacking**

- ❑ **Websites hacking**

  *According servers securities levels it can be said that hackers knew passwords

- ❑ **Spamming of Email addresses**

According to many facts, It seems that cyber attacks were planned before the actual war started, analyzes made by Military experts was that actual war was also planned a long time before !



08.08.2008, 06:32 #62

sabe
Участник форума
Регистрация: 16.03.2007
Адрес: http://hack.this.name
Сообщения: 299
Провел на форуме:
1 неделю 2 дня

Репутация: Эксперт (2/430) ±

Грузинские Сайты в тему:

http://www.tbilisi.gov.ge/index.php?Post=1%22%3E%20%3Cscript%3Ealert(/suki/)%3C/script%3E&sec_id=337&lang_id=DEU

Aversi.ge

Цитата:

```
http://www.aversi.ge/main.php?lang=geo&id=-1+UNION+SELECT+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15 ,version(),17,18,19,20,21,22,23/*
```

Presa.ge

Цитата:

```
http://presa.ge/index.php?text=news&i=-1+union+select+1,2,concat_ws(0x3a,table_name),4,5,
6,7,8,9,10,11+from+information_schema.tables+limit +17,1--
```

5 ver. tables

Цитата:

```
http://presa.ge/index.php?text=news&i=-1+union+select+1,2,concat_ws(0x3a,user_username,us
er_password),4,5,6,7,8,9,10,11+from+users--
```

Ssa.gov.ge

Цитата:

```
http://www.ssa.gov.ge/index.php?id=69&mid=-1+union+select+1,2,3,4,5,6,7,8,9,version(),11,12,1 3,14,15,16,17,18,19,20,21,22,23,24,25
```

Bank Troubles

- Georgian biggest bank TBC was under attack starting from early morning of the 9th of August. Attack overloaded firewall. The ATM and payment terminal availability issues were partially caused by the overloaded firewall.

- When the attacks started, the National Bank of Georgia ordered all banks to temporarily cease all the electronic services (bank websites and internet banking) This order did not concern services needed to do transaction inside and between the banks.

What kind ties Estonian and Georgian events have

Ties

Russians where involved
Estonians where involved

Attack Patterns

Government

Estonian Case

- www.president.ee
- www.valitsus.ee
- www.mfa.ee

And so on….

Georgian Case

- www.president.gov.ge
- www.mfa.gov.ge
- www.government.gov.ge
- www.parliament.ge
- www.mod.gov.ge
- www.nbg.gov.ge
- www.cec.gov.ge
- www.mof.ge
- www.abkhazia.gov.ge

And so on….

News

Estonian Case

- ❑ www.postimees.ee
- ❑ www.delfi.ee
- ❑ www.epl.ee

And so on….

Georgain Case

- ❑ www.rustavi2.com
- ❑ www.interpress.ge
- ❑ www.civil.ge
- ❑ www.forum.ge
- ❑ www.apsny.ge

And so on….

Everything else

Estonian Case

- www.ebs.ee
- www.tpu.ee
- est.ttu.ee
- www.infoatlas.ee
- www.zzz.ee

And so on….

Georgain Case

- www.internet.ge
- www.geres.ge
- www.chca.org.ge
- www.presa.ge
- www.museum.ge

And so on….

Differences

- Each attack is in some ways unique
- New attack strategies
- Connection to physical events

Money

Estonian Case

- www.hansa.ee
- www.seb.ee
- www.sampo.ee
- www.krediidipank.ee

Georgian Case

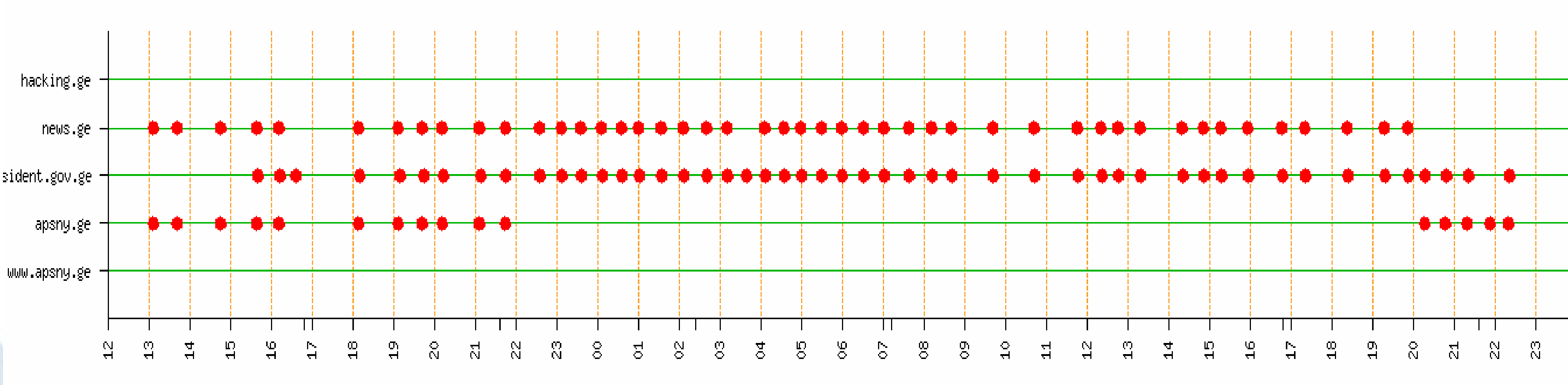
- www.nbg.gov.ge
- www.tbcbank.ge
- www.republic.ge
- www.vtb.com.ge

Things to wonder about

From Shadowserver, sampling of previous DDoS targets from the same botnets involved in the Georgia attacks:

www.in-bank.net
carder.biz
Divaescort.com
payclubs.biz
night-fairy.com
vodkaescort.net
cc-hack.eu
igame.ru
i-german.net

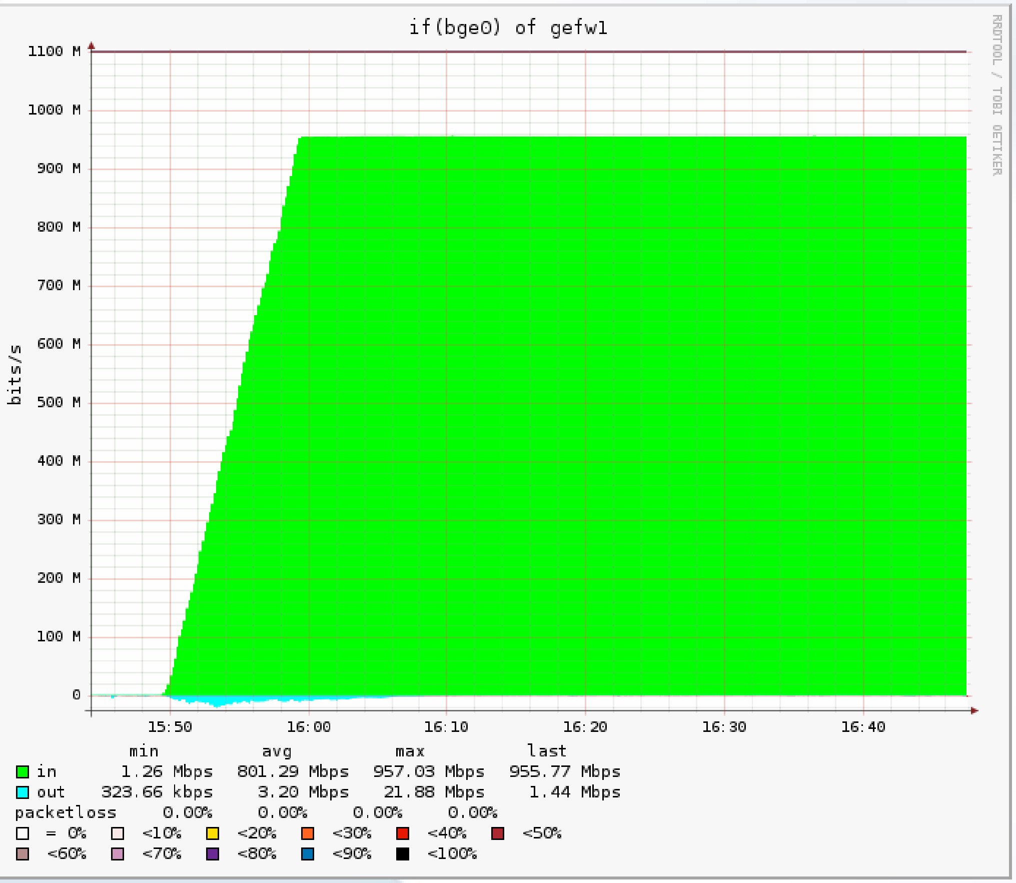
Things to wonder about



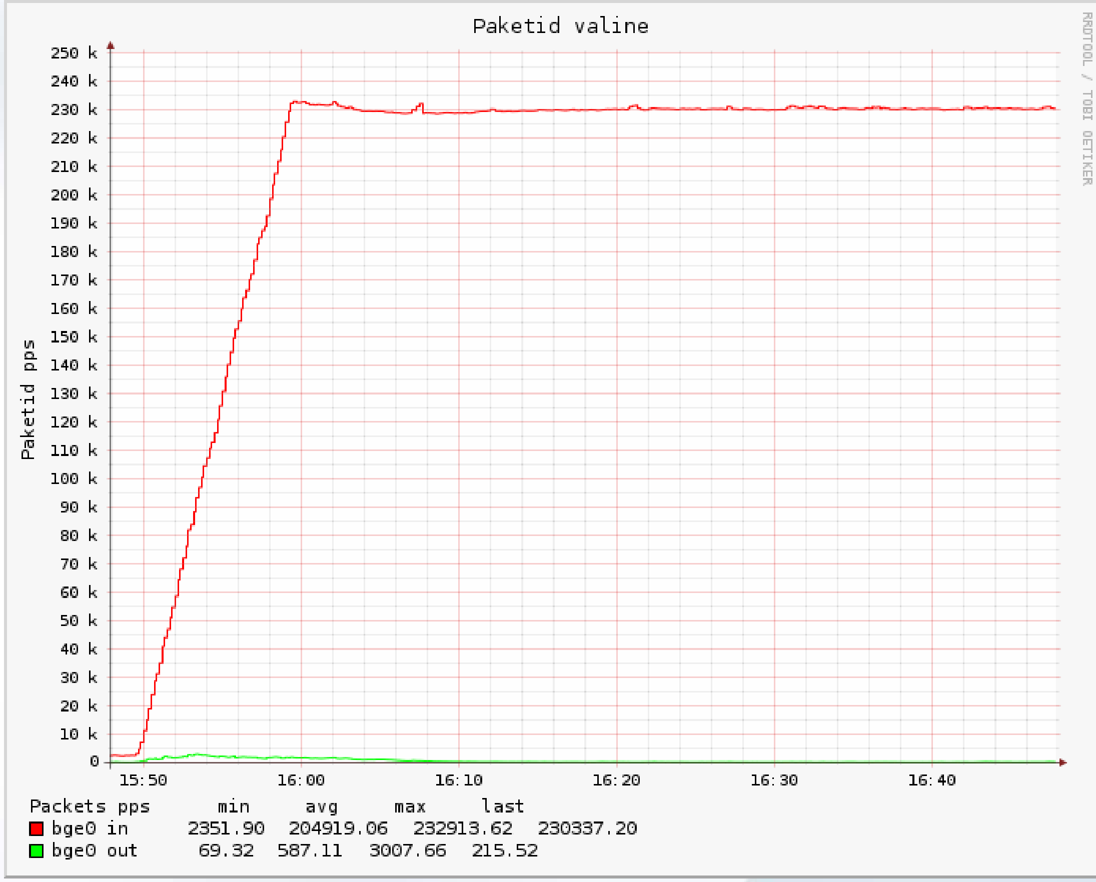
Information courtesy of shadowserver

How media can influents the world

Attacks of civil.ge after news that Estonia is in business of site hosting

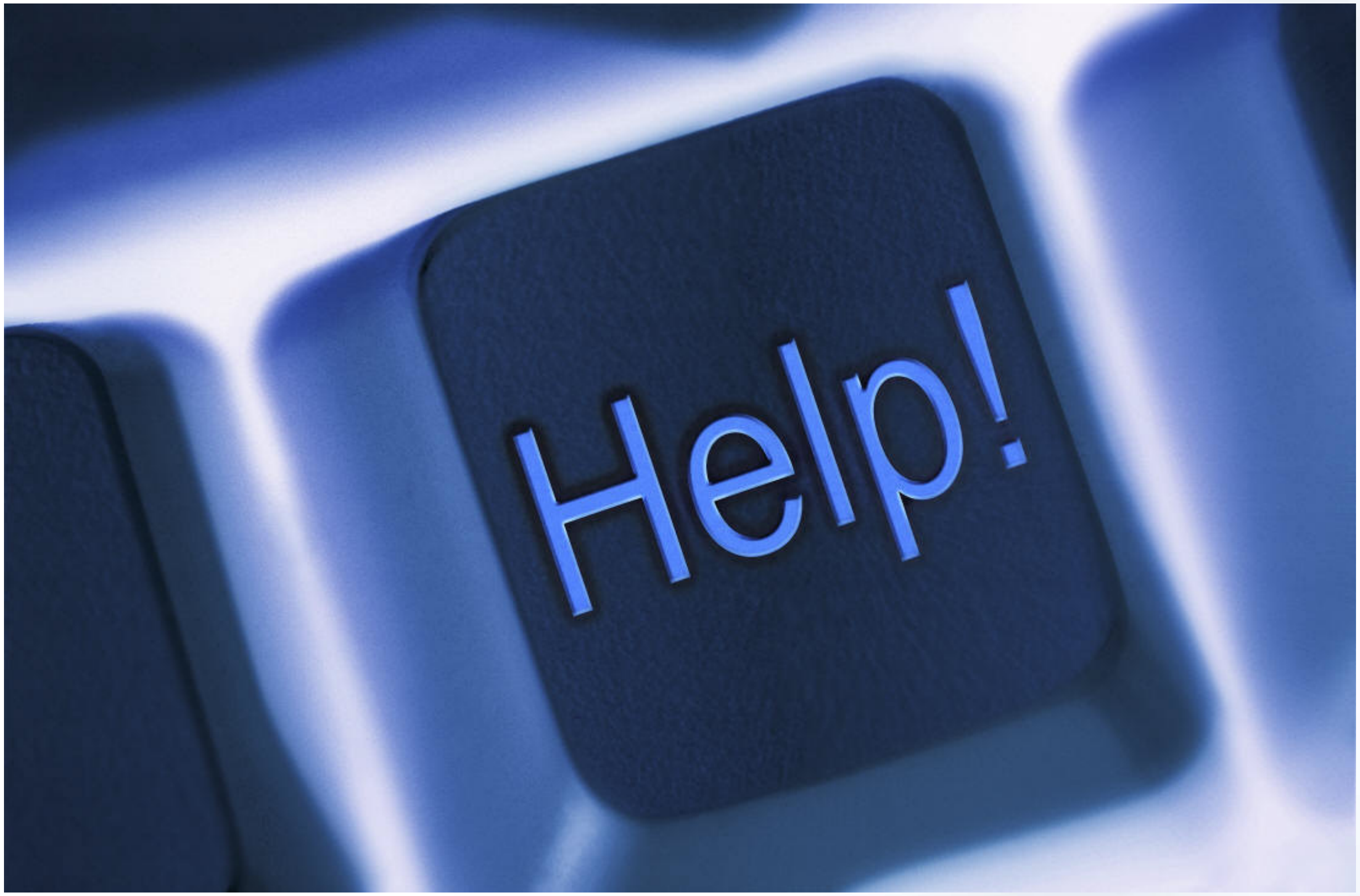


```
                 min          avg          max         last
🟩 in        1.26 Mbps  801.29 Mbps  957.03 Mbps  955.77 Mbps
🟦 out     323.66 kbps    3.20 Mbps   21.88 Mbps    1.44 Mbps
packetloss     0.00%        0.00%        0.00%        0.00%
□  = 0%   □  <10%   🟨 <20%   🟧 <30%   🟥 <40%   🟫 <50%
🟫 <60%   □  <70%   🟪 <80%   🟦 <90%   ⬛ <100%
```



```
Packets pps      min        avg         max        last
🟥 bge0 in     2351.90  204919.06  232913.62  230337.20
🟩 bge0 out      69.32     587.11    3007.66     215.52
```

How the incidents where handled



Estonian case

With little help from my Freiends

- Kurtis
- Gorazd
- cert.fi

Georgian Case

CERT Georgia is part of the Georgian Research and Educational Networking Association – GRENA and serving its users. As there are no other CERT teams in Georgia, during the attacks CERT-GE undertook obligation to operate as national CERT and coordinate attacks mitigation.

CERT-GE contacted Georgian ISPs and other organizations, created a mailing list in order to facilitate communication and exchange of all needed information. This proved to be very successful, as all interested parties started sending a large amount of information reporting incidents.

As this information was huge and geographical distribution of attacks was quite wide, it was impossible to make quick analysis and proper reaction. CERT-GE contacted our partner CERT-Polska (Poland) which offered its help in preventing and filtering attacks; as a quick action they distributed information on attacks to more than 180 CERT teams and other security related bodies all over the world.

What we can learn

Obvious things for this community

- ❑ Have a community not only this one but with in your country
- ❑ Every conflict situation will be support by cyber attacks with high probability
- ❑ Cyber attacks can be done by hands of ordinary citizens accessing internet
- ❑ Attackers learned how to better mobilize masses for participation in the attacks, combination of tactics increased result of the attacks.
- ❑ Security is not for competition

Not so obvious things

❑ Against network you can fight efectivly only with neetwork so organization has to be network avoiding hierarchies and "central point of reporting"

❑ Communication has to be real time and all involved online

❑ m,b&g are also Critical infrastructure

❑ Try to think out side box and make mistakes ☺

To build trusted network
we can always find place and time to have nice meal , drink bear , wine or
sakke and make friends

something to read :
http://www.sans.org/reading_room/whitepapers/leadership/rss/beer_the_key_ingredient_to_team_development_33104
And give something back to community.