

CERT-GOV-GE

Activities & Services

Tbilisi, Georgia 2014
CERT-GOV-GE Manager
David Kvatadze

MINISTRY OF JUSTICE OF GEORGIA

DATA EXCHANGE
AGENCY



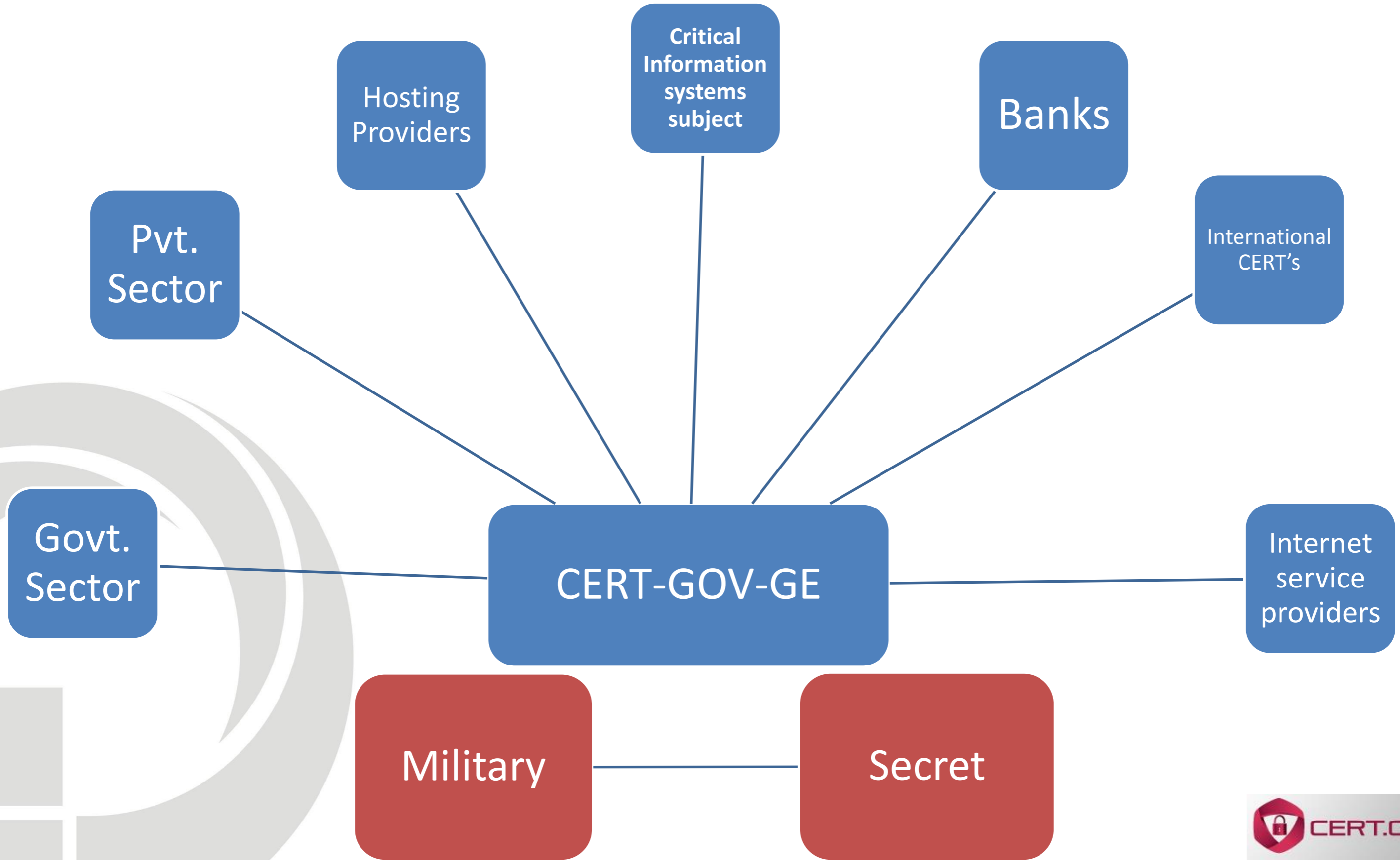
www.dea.gov.ge

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.

CERT-GOV-GE Constituency



CERT-GOV-GE Services

Services:

- IP address monitoring service portal;
- Incident Handling;
- Penetration test
- Netflow Sensors (Nfdump & Nfsen);
- Web-Site Intrusion Detection (Threat Factor);
- Blacklist service;
- Safe DNS Georgia;
- Training on Cyber Incident Handling;
- Check My IP;

Other activities:

- Georgian Information Security Forum (Abuse Forum);
- Information Security Awareness;



CERT.GOV.GE

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.

Certifications:



All Our Team members are Certified by SANS GIAC.

Plans:



All Our Team members have plan to pass SANS GSNA exam.

CERT-GOV-GE

Plans for the 2015 year :

EGC Group

CERT.gov.ge is planning to become a member of European Government CERTs (EGC) group.



CERT.gov.ge is planning to become a certified member of Trusted Introducer.



It is also planned to become a member of APCERT.

CERT-GOV-GE (Computer Emergency Response Team)

Our Partners:



www.impact-alliance.org



www.trusted-introducer.org



www.nato.int



www.shadowserver.org



www.team-cymru.org



www.arbornetworks.com



www.arakis.pl



www.eset.com



www.microsoft.com



www.symantec.com



<http://www.cert.pl/>



www.cert.at



www.cert.ee/



www.quarantainenet.nl



Information Provided Daily About Infected IP Adresse:



Infected 10 000 IP Addresses



Infected 20 000 IP Addresses



Infected 1 500 IP Addresses



Infected 500 IP Addresses

network security incident exchange



Infected 100 IP Addresses



CLEAN-MX

15-20 Phishings

25-30 Deface Web-Sites

15-20 Malware Sites





The Hacker News

Truth is the most powerful weapon against Injustice

Albania is the most Malware infected Nation



<http://thehackernews.com/2012/03/albania-is-most-malware-infected-nation.html>

Researchers at Security firms Norman and Microsoft Analyse data from their security products to find that Albania is the most Malware infected Nation, with 65% of scanned computers reporting infections. Report Most Infected Countries are South Korea, Guatemala, Vietnam, Indonesia, Argentina, Thailand, Georgia, the Philippines, Algeria, Venezuela, Lithuania and Pakistan according to Norman Report.

CERT-GOV-GE Services

➤ IP address monitoring portal

IP მისამართების მონიტორინგის პორტალი გამარჯობათ Administrator [გამოსვლა]
პაროლის შეცვლა

მთავარი | IP მონიტორინგი | ორგანიზაციების სია | მომხმარებლები

IP მონიტორინგის ცხრილი ipMonitor

Arakis სულ ნაპოვნია 1 ჩანაწერი

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

Shadow Sinkhole სულ ნაპოვნია 5 ჩანაწერი

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

Shadow BotNet სულ ნაპოვნია 2 ჩანაწერი

IP მისამართი	ორგანიზაცია	დაინფიცირების ტიპი	სმარტფონის ცენტრი	მარტფონის ცენტრის პორტი	თარიღი	
77.92.224.114	XXXXXXXXXXXXXXXXXXXXXXXXXXXX	salinity-p2p			4/11/2013 10:56:12 AM	
77.92.224.114	XXXXXXXXXXXXXXXXXXXXXXXXXXXX	zeus-p2p			4/11/2013 10:50:12 AM	

Team Cymru სულ ნაპოვნია 3 ჩანაწერი

IP მისამართი	ორგანიზაცია	დაინფიცირების ტიპი	თარიღი	
77.92.224.121	XXXXXXXXXXXXXXXXXXXXXXXXXXXX	openresolvers	2/7/2013 6:	

CERT-GOV-GE Services

➤ IP address monitoring portal

IP მისამართების მონიტორინგის პორტალი გამარჯობათ Administrator [გამოსვლა] პაროლის შეცვლა

- მთავარი
- IP მონიტორინგი**
- ორგანიზაციების სია
- მომხმარებლები

IP მონიტორინგის ცხრილი








1/1/2012 6/12/2013 XXXXXXXXXXXXXXXXXXXXXXXXXXXX მიემა



Araki სულ ნაპოვნია 1 ჩანაწერი

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

Shadow Sinkhole სულ ნაპოვნია 5 ჩანაწერი

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

Shadow BotNet სულ ნაპოვნია 2 ჩანაწერი

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

Team Cymru სულ ნაპოვნია 3 ჩანაწერი

IP მისამართი	ორგანიზაცია	დაინფიცირების ტიპი	თარიღი	
77.92.224.121	XX	openresolvers	2/7/2013 6:...	

CERT-GOV-GE Services

➤ IP address monitoring portal

IP მისამართების მონიტორინგის პორტალი გამარჯობათ Administrator [გამოსვლა]
პაროლის შეცვლა

თქვენი IP მონიტორინგის პორტალი

თარიღი: 6/12/2013

საფილტრები: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

მიემა

Araki სულ ნაპოვნია 1 ჩანაწერი

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

Shadow Sinkhole სულ ნაპოვნია 5 ჩანაწერი

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	salinity	6/19/2012 6:57:43 AM
77.92.224.114	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	salinity	6/13/2012 5:41:26 AM

Shadow BotNet სულ ნაპოვნია 2 ჩანაწერი

IP მისამართი	ორგანიზაცია	დაინფიცირების ტიპი	სმარტფონის ცენტრი	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 სულ ნაპოვნია 3 ჩანაწერი

IP მისამართი	ორგანიზაცია	დაინფიცირების ტიპი	თარიღი
77.92.224.121	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	openresolvers	2/7/2013 6:

CERT-GOV-GE Services

➤ IP address monitoring portal

IP მისამართების მონიტორინგის პორტალი

გამარჯობათ Administrator [გამოსვლა] პაროლის შეცვლა

თქვენი IP მონიტორინგის პორტალი

IP მონიტორინგის პორტალი

თარიღი: 6/12/2013

XXXXXXXXXXXXXXXXXXXX

მიემა

ipMonitor

სულ ნაპოვნია 1 ჩანაწერი

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

Shadow Sinkhole

სულ ნაპოვნია 5 ჩანაწერი

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

Shadow BotNet

სულ ნაპოვნია 2 ჩანაწერი

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

Team Cymru

სულ ნაპოვნია 3 ჩანაწერი

IP მისამართი	ორგანიზაცია	დაინფიცირების ტიპი	თარიღი
77.92.224.121	XX	openresolvers	2/7/2013 6:

CERT-GOV-GE Services

➤ IP address monitoring portal

IP მისამართების მონიტორინგის პორტალი გამარჯობათ Administrator [გამოსვლა]
პაროლის შეცვლა

თქვენი IP მონიტორინგის პორტალი

IP მისამართი: | ორგანიზაცია: | საფრთხის დონე: | მიემა: | თარიღი: |

სულ ნაპოვნია 1 ჩანაწერი

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

Shadow Sinkhole სულ ნაპოვნია 5 ჩანაწერი

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

Shadow BotNet სულ ნაპოვნია 2 ჩანაწერი

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

Team Cymru სულ ნაპოვნია 3 ჩანაწერი

IP მისამართი	ორგანიზაცია	დაინფიცირების ტიპი	თარიღი
77.92.224.121	XX	openresolvers	2/7/2013 6:...

CERT-GOV-GE Services

➤ IP address monitoring portal

IP მისამართების მონიტორინგის პორტალი გამარჯობათ Administrator [გამოსვლა]
პაროლის შეცვლა

თქვენი IP მონიტორინგის პორტალი

Araki: 12 6/12/2013 XXXXXXXXXXXXXXXXXXXXXXX მიემა

სულ ნაპოვნია 1 ჩანაწერი

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

Shadow Sinkhole სულ ნაპოვნია 5 ჩანაწერი

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


Shadow BotNet სულ ნაპოვნია 2 ჩანაწერი

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

Team Cymru სულ ნაპოვნია 3 ჩანაწერი

IP მისამართი	ორგანიზაცია	დაინფიცირების ტიპი	თარიღი
77.92.224.121	XX	openresolvers	2/7/2013 6:

**12 Million Infected IP,s
200 thousand unique IP's**

 CERT.GOV.GE

Check My IP

← → ↻ 🏠 www.dea.gov.ge/?action=page&p_id=133&lang=geo



შთავარი | საიტის რუკა | კონტაქტი | RSS

GEO ENG

ძიება...

ჩვენს შესახებ

მომსახურება

CERT.GOV.GE

საკანონმდებლო ბაზა

დოკუმენტები

პარტნიორები

საინფორმაციო ფურცელი

TWINNING

GITI

Check My IP

Your IP address is: 146.255.225.150

Infection type: Zeus

[Detailed Information](#)



ელექტრონული
მმართველობა

მონაცემთა გაყვლის
ინფრასტრუქტურა

ინფორმაციული
უსაფრთხოება

სტატიები

11 აპრილი 2012
SPAM - სპამი

03 თებერვალი 2012
ფიშინგი

26 ივლისი 2011
საზღვრის უკანა-ინტერნეტ ქსელის უსაფრთხოება

25 ივლისი 2011
Malware – „ბოროტი პროგრამა“

[ინილეთ ყველა](#)

Check My IP

← → ↻ 🏠 📄 www.dea.gov.ge/?action=page&p_id=133&lang=geo



შთავარი | საიტის რუკა | კონტაქტი | RSS

GEO ENG 🏠

ძიება...

ჩვენს შესახებ

მომსახურება

CERT.GOV.GE

საკანონმდებლო ბაზა

დოკუმენტები

პარტნიორები

საინფორმაციო ფურცელი

TWINNING

GITI

Check My IP

- **Your IP address is:** 146.255.225.150
- **Infection type:** Zeus
- **Short description of infection type:** Zeus is a Trojan horse that steals banking information by Man-in-the-browser keystroke logging and Form Grabbing. Zeus is spread mainly through drive-by downloads and phishing schemes. First identified in July 2007 when it was used to steal information from the United States Department of Transportation, it became more widespread in March 2009. In June 2009, security company Prevx discovered that Zeus had compromised over 74,000 FTP accounts on websites of such companies as the Bank of America, NASA, Monster.com, ABC, Oracle, Play.com, Cisco, Amazon, and BusinessWeek.
- **Command & Control:** 89.232.125.112
- **Date:** 27 მაისი 2013 11:23:15 PM



ელექტრონული
მმართველობა

მონაცემთა გაყვლის
ინფრასტრუქტურა

ინფორმაციული
უსაფრთხოება

სტატიაები

11 აპრილი 2012
SPAM - სპამი

03 თებერვალი 2012
ფიშინგი

26 ივლისი 2011
საზღვარის უკანა-ინტერნეტ ქსელის უსაფრთხოება

25 ივლისი 2011
Malware – „მოროტი პროგრამა“

ინილუა ვველა

Check My IP

← → ↻ 🏠 www.dea.gov.ge/?action=page&p_id=133&lang=geo



შთავარი | საიტის რუკა | კონტაქტი | RSS

GEO ENG



ძიება...



ჩვენს შესახებ

მომსახურება

CERT.GOV.GE

საკანონმდებლო ბაზა

დოკუმენტები

პარტნიორები

საინფორმაციო ფურცელი

TWINNING

GITI

Check My IP

Your IP address is: 146.255.225.150

Infection type: not found



ელექტრონული
მმართველობა

მონაცემთა გაყვლის
ინფრასტრუქტურა

ინფორმაციული
უსაფრთხოება

სტატიები

11 აპრილი 2012
SPAM - სპამი

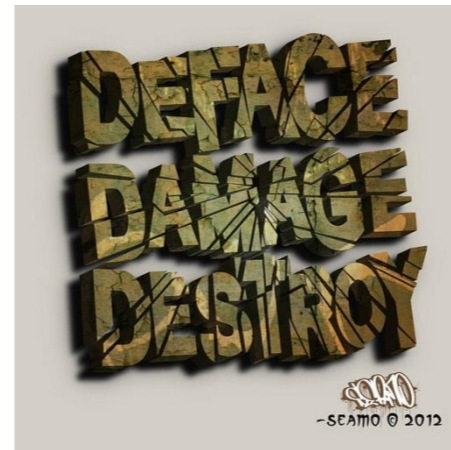
03 თებერვალი 2012
ფიშინგი

26 ივლისი 2011
საზღვარის უკანა-ინტერნეტ ქსელის უსაფრთხოება

25 ივლისი 2011
Malware – „ბოროტი პროგრამა“

ინილეთ ყველა

➤ Incident Handling



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

Contact: incidents@dea.gov.ge

CERT-GOV-GE Services

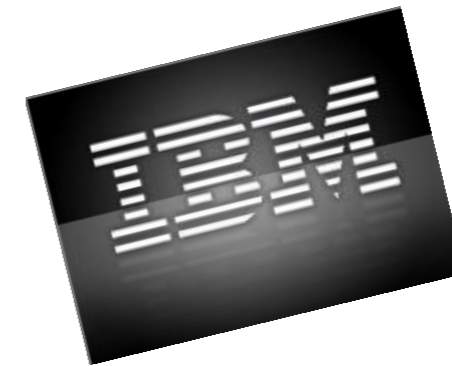
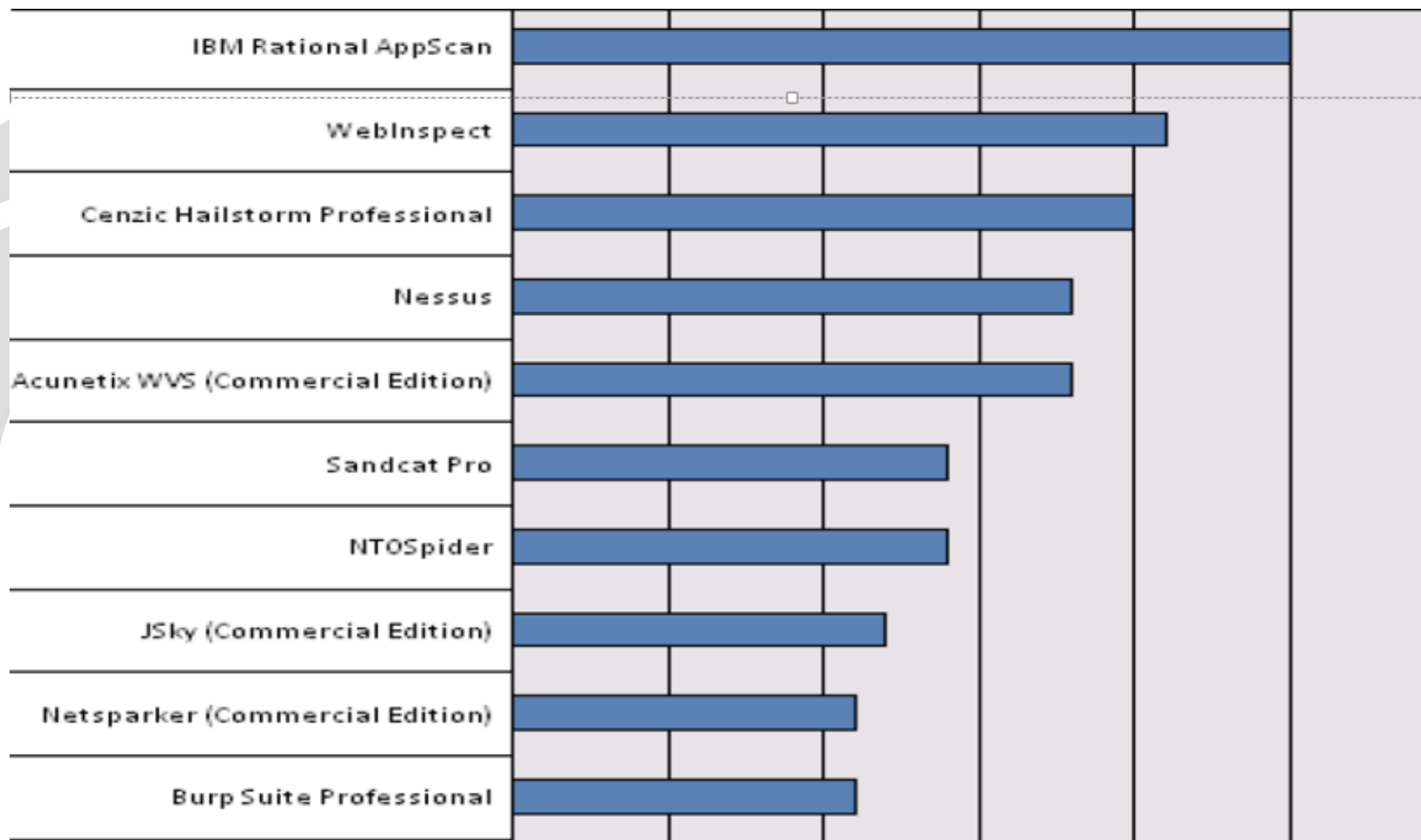
➤ Penetration test

Top 10 commercial tools



OWASP

The Open Web Application Security Project



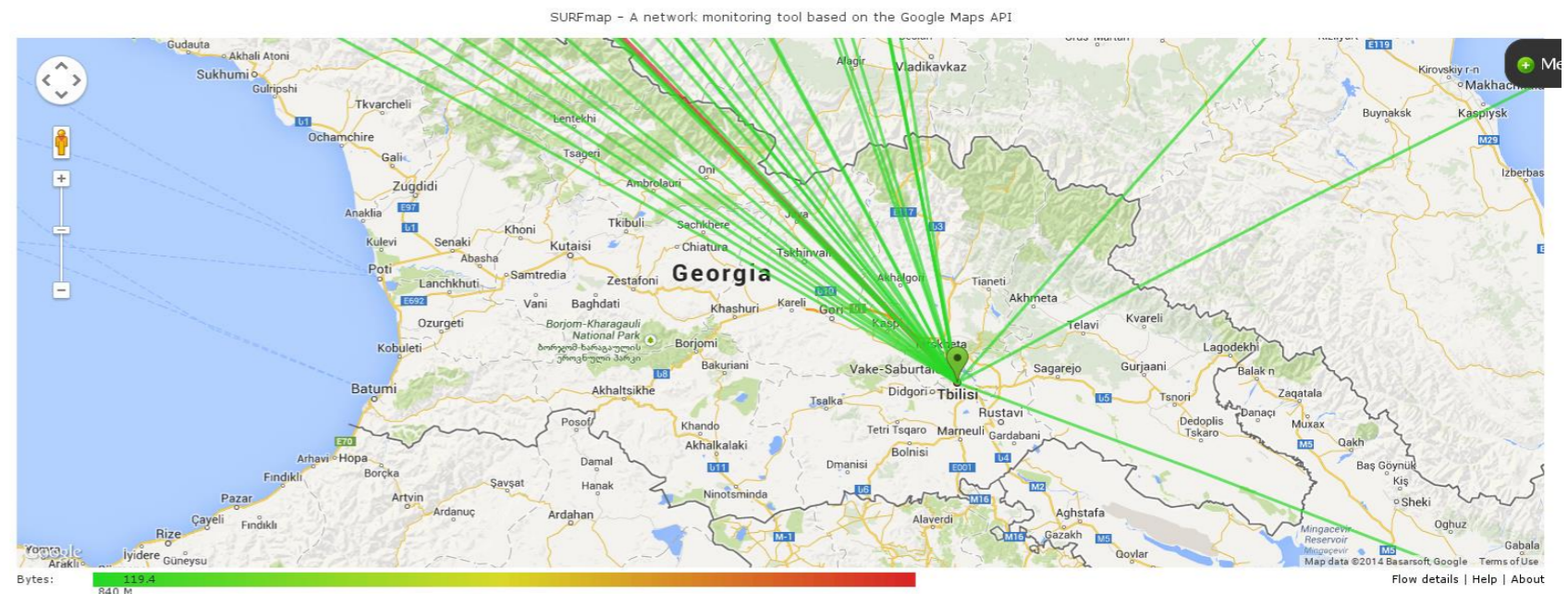
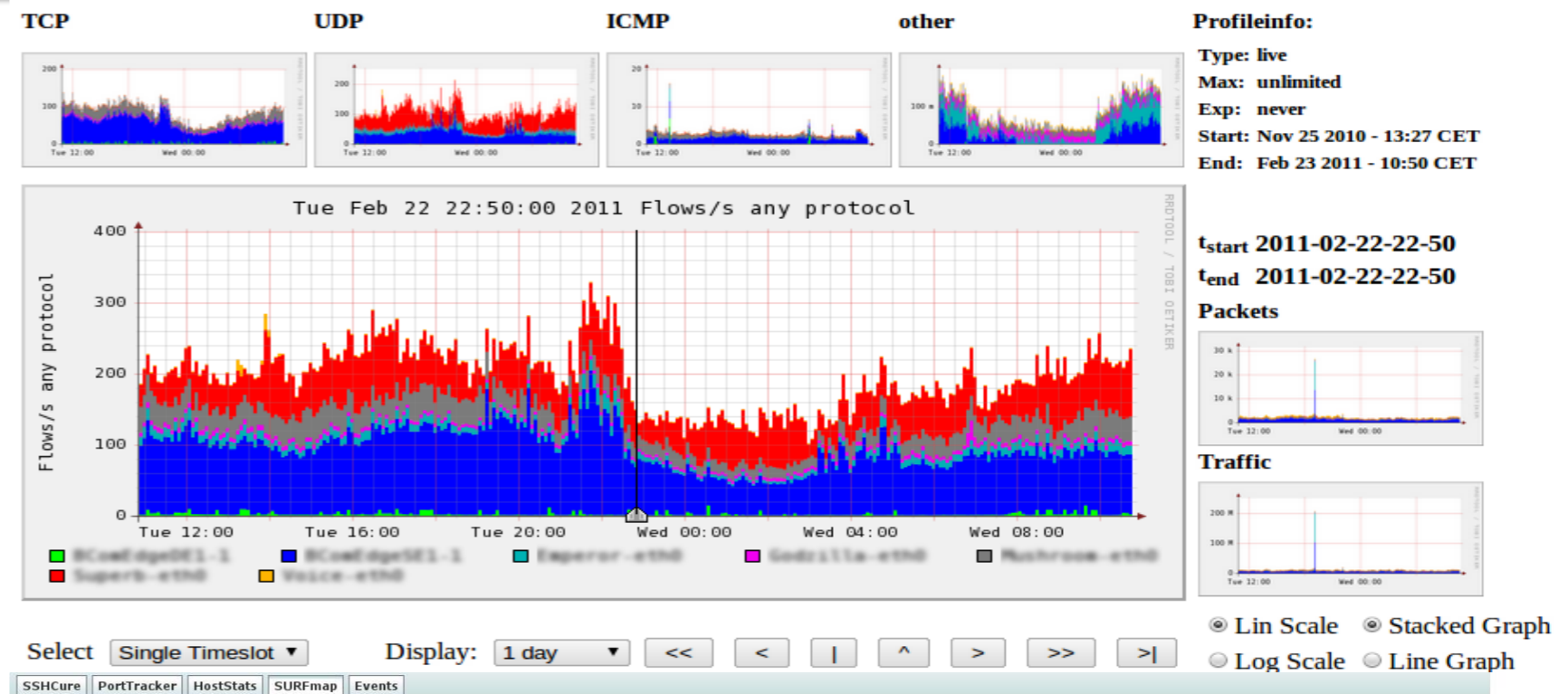
CERT-GOV-GE Services

➤ NetFlow Sensors (NfDump & NfSen)

Analyze NetFlow Data For Security.

Detects:

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

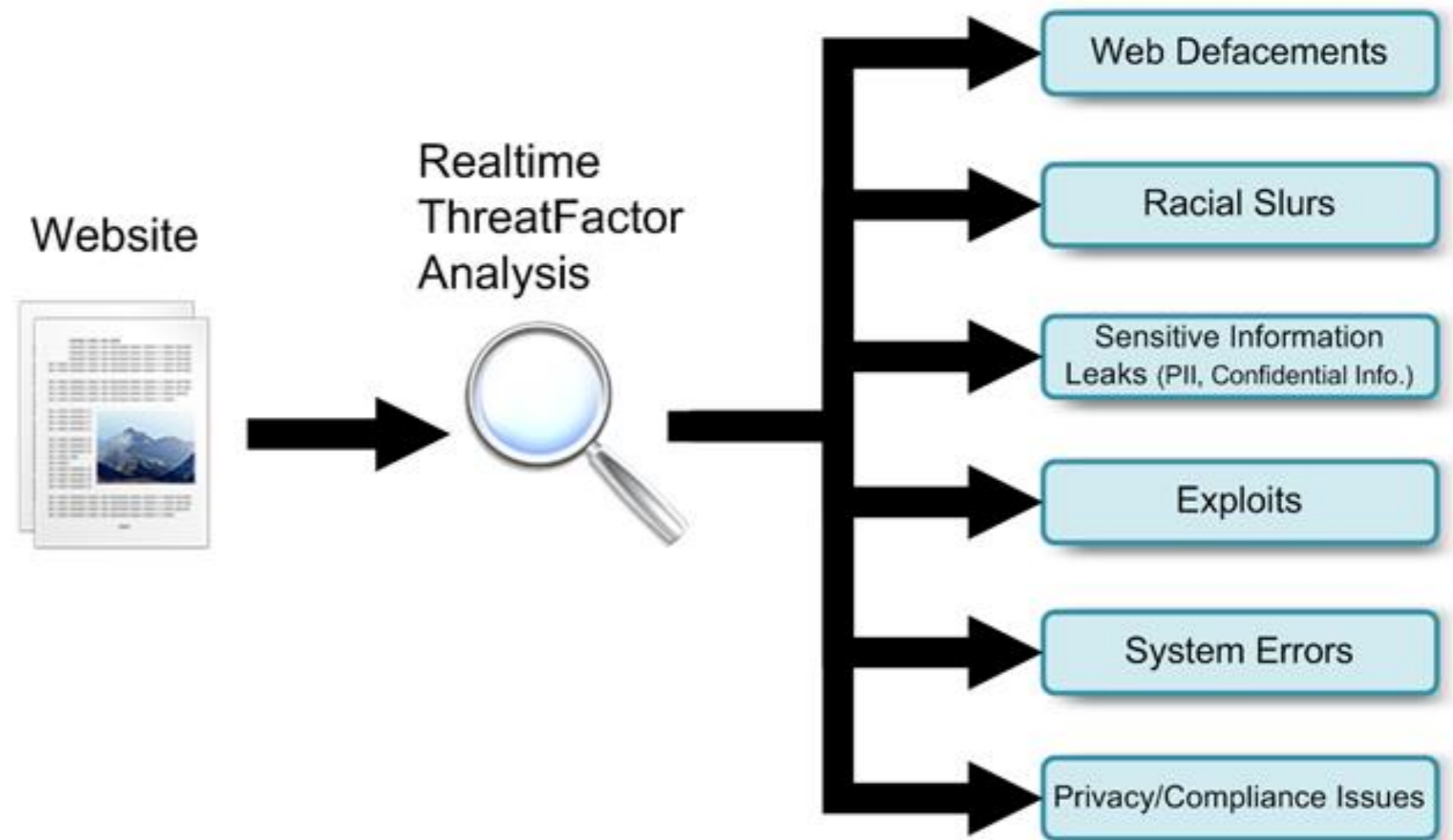


➤ Website Intrusion Detection (ThreatFactor)

Open Source Project.

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

Custom Rule Based Detection.



➤ Blacklist Service

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



CERT-GOV-GE Services

➤ 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



➤ Training on Cyber Incident Handling



Software Engineering Institute
Carnegie Mellon

NATO SPS Programme

Cyber Defence Training for IT Professionals

- **Afghanistan**
- **Moldova**
- **Macedonia**
- **Montenegro**
- **Azerbaijan**



CERT-GOV-GE other activities

➤ Georgian Information Security Forum (Abuse Forum)



**2014
FIRST
Regional
Symposium**



**Tbilisi, Georgia
October 13-16, 2014**

Cyber EXE Georgia 2014 – CEG14

CYBER-EXE 2014 GEORGIA

24 September, 2014

CERT-GOV-GE other activities

➤ Georgian Information Security Forum (Abuse Forum)



CYBER-EXE GEORGIA 2014



CERT-GOV-GE other activities

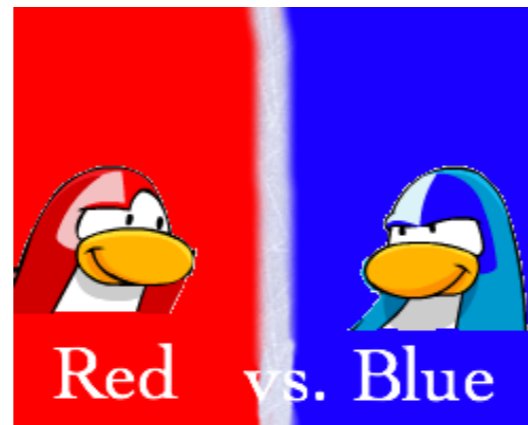
➤ Georgian Information Security Forum (Abuse Forum)



Red Team

- CERT-GOV-GE
- COMCERT.pl

CYBER-EXE GEORGIA 2014



CERT-GOV-GE other activities

➤ Georgian Information Security Forum (Abuse Forum)



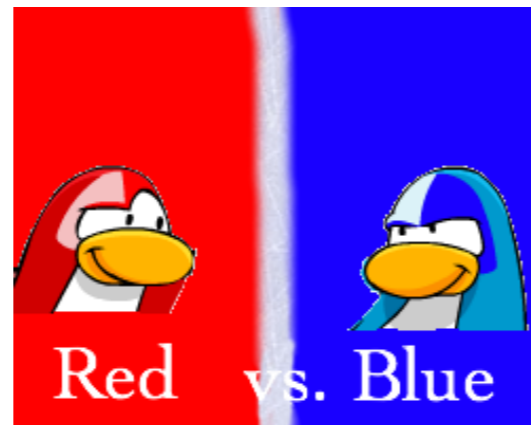
Red Team

- CERT-GOV-GE
- COMCERT.pl

CYBER-EXE GEORGIA 2014

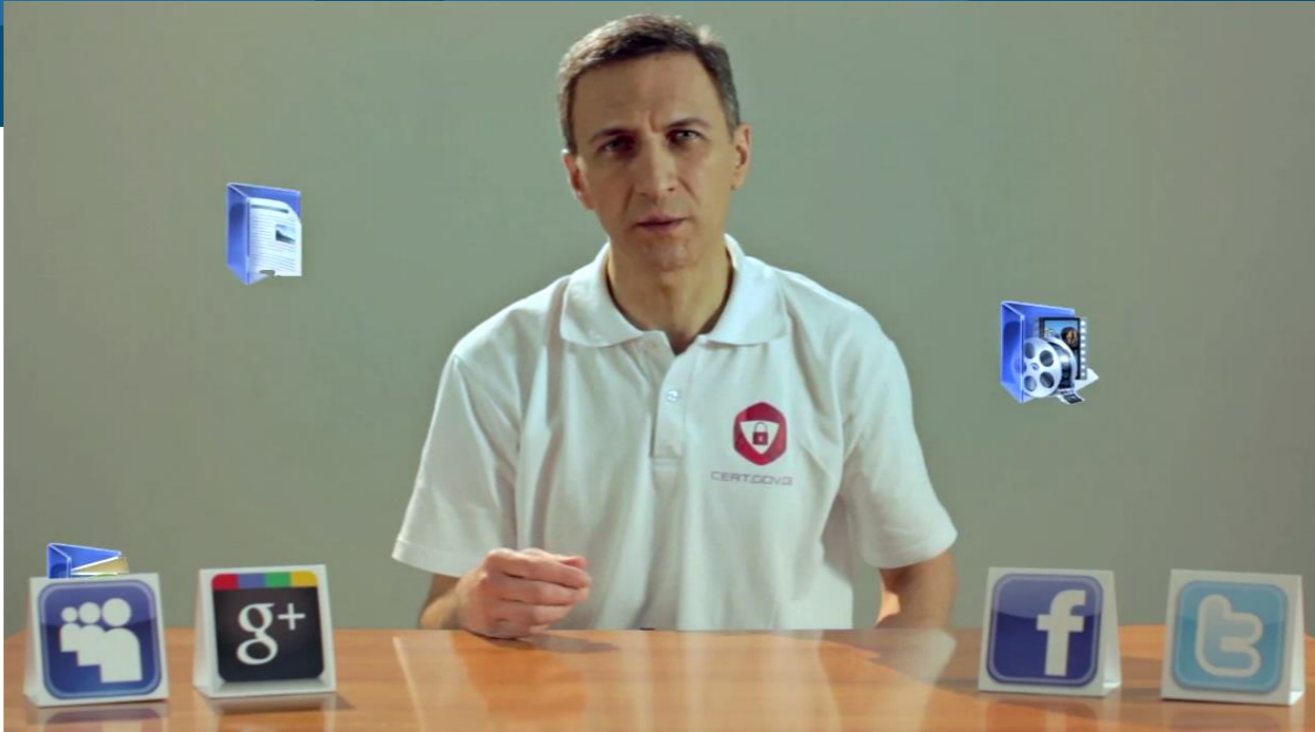
Blue Team

- Education Management Information System
- National Public Registry
- Ministry of Labour Health and Social Affairs of Georgia
- MagtiCom
- Bank of Georgia
- Georgian Research and Educational Network Association Grena
- Ministry of Internal Affairs
- National Bank of Georgia
- Cyber Security Bureau
- Smart Logic
- state chancelary
- Geocell
- VTB Bank
- Ministry of Finance of Georgia
- Public Service Development Agency
- Free University of Tbilisi



Information Security Awareness:

განიკი
May 2012



მდომობერი
October 2012





www.facebook.com/certgovge

You are posting, commenting, and liking as CERT.GOV.GE — Change to David Kvatadze

CERT.GOV.GE Timeline Now

Admin Panel

Ads Manager

Like · Comment · Share

150 people saw this post

Boost Post

CERT.GOV.GE February 28

გატეხილია drums.ge ვებ-გვერდი, ვებ-გვერდზე მოხდა ეგრედწოდებული "deface".
Defaced Site - <http://www.drums.ge/>
Date - 2013-02-27 20:24:05 CET
IP Address - 91.212.213.2

qd56d5e8d25s.fdsf456e6d5sde8d56s4d.d545d4e84d5d.d89626/5S
F8Z650/a607a763a17a64e97b8979c77687991e/login.htm



Like · Comment · Share

1

133 people saw this post

Boost Post

CERT.GOV.GE February 28

გატეხილია soa.gov.ge ვებ-გვერდი, ვებ-გვერდზე მოხდა ეგრედწოდებული "deface".



See Your Ad Here



David Kvatadze



CERT.GOV.GE

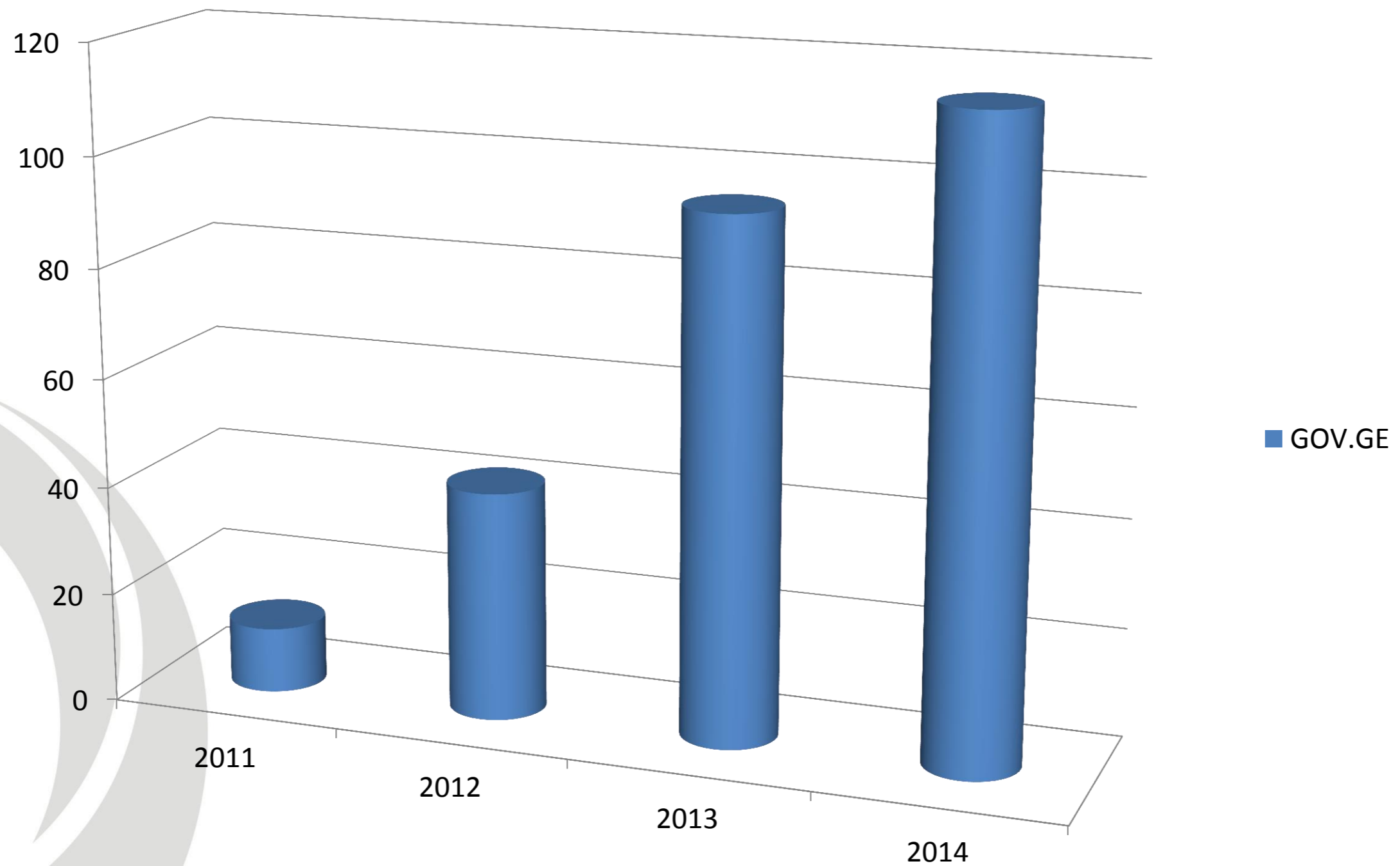
Statistics



- We are receiving and analyzing information about **20000** infected Georgian IP addresses from our international partner organizations on a daily basis.
- We shut down approximately **20** phishing sites that are located in Georgian web space on monthly basis.
- Hackers deface approximately **25** sites in Georgian cyber space on monthly basis.
- We receive information about **35** infected web sites which are located in Georgian web space on monthly basis.

Statistics

GOV.GE



CERT-GOV-GE

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



Thank You!

Questions?



საქართველოს იუსტიციის სამინისტრო

პონაქაშოთა გაცვილის
სააგენტო

