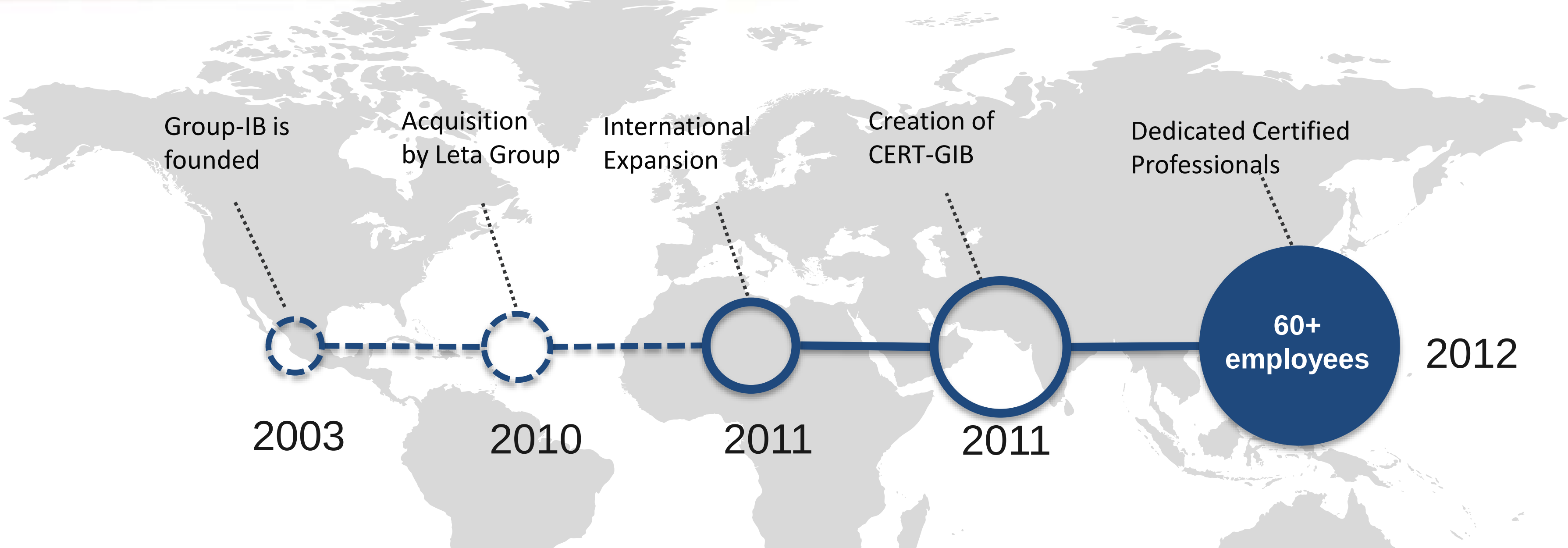
CYBER CRIMES INVESTIGATION • CYBER CRIMES INVESTIGATION •

GROUP IB

Security and cooperation in terms of cyber threats in Runet

Group-IB


Group-IB is founded

2003

Acquisition by Leta Group

2010

International Expansion

2011

Creation of CERT-GIB

2011

Dedicated Certified Professionals

60+ employees

2012

Stages of Sustainable Solid Development

Leader on the Russian market
The first and only company in the CIS providing comprehensive services in investigating IT security incidents.

Service package
Pre-incident consulting;
Response;
Forensics;
Investigation;
Legal support;
Post-incident consulting.

Skolkovo resident
The CyberCop project, an integrated system for counteracting cybercrime.

First 24/7 CERT in Eastern Europe
CERT-GIB is the first private Computer Emergency Response Team in Russia..

Group-IB: Services provided

- Computer Forensics
- Malware investigation
- Cyber crimes investigation
- Brand Protection and associated risk mitigation
- DDoS Protection and mitigation
- Botnet monitoring

The only non-governmental organization providing cybercrime investigation and mitigation services in Russia.

Our Partners

✓National and private CERTs in over 55 countries

✓Major Antivirus Editors

✓Computer forensic and IT-security solution providers worldwide

✓US and European Academic Institutions

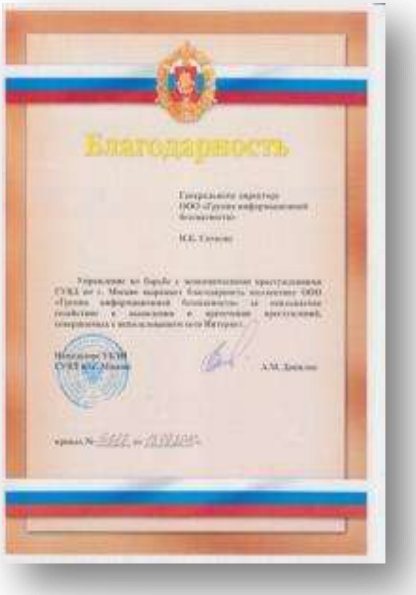
✓International Forensic and Anti-cybercrime community memebers

✓Association of Certified Fraud Examiners (ACFE)

✓LEA and Special Services: FBI, US Secret Service

International Information Systems Forensics Association
iisfa
High Technology Crime Investigation Association
HTCIA
International Society of Forensic Computer Examiners
MCCE
The Institute of Computer Forensic Professionals
ICFP
POLCYB
ACFE
Association of Certified Fraud Examiners
SOURCEfire
GuardianEdge
trustedPARTNER

LE cooperation



Благодарность

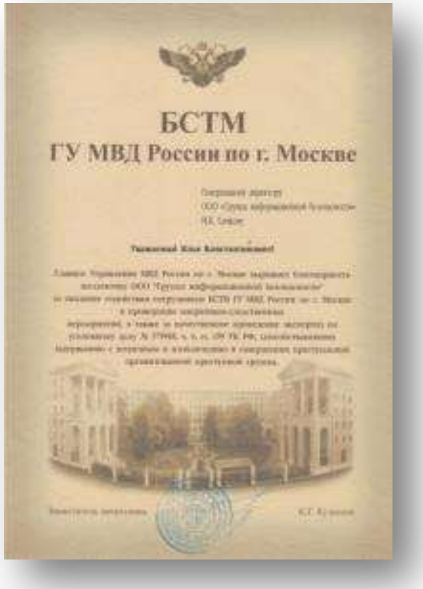
Генеральному директору
ООО «Группа информационной безопасности»

И.К. Сачкову

Управление по борьбе с экономическими преступлениями ГУВД по г. Москве выражает благодарность коллективу ООО «Группа информационной безопасности» за оказанное содействие в выявлении и пресечении преступлений, совершенных с использованием сети Интернет.

Начальник УБЭП ГУВД по г. Москве А.М. [illegible]

приказ № [illegible] от [illegible]



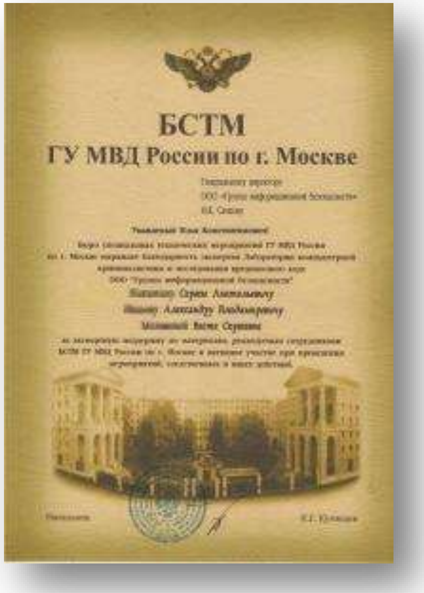
БСТМ
ГУ МВД России по г. Москве

Генеральному директору
ООО «Группа информационной безопасности»
И.К. Сачкову

Уважаемый Илья Константинович!

Главное Управление МВД России по г. Москве выражает благодарность коллективу ООО "Группа информационной безопасности" за оказание содействия сотрудникам БСТМ ГУ МВД России по г. Москве в проведении оперативно-розыскных мероприятий, а также за качественное проведение экспертиз по уголовному делу № [illegible] [illegible] организованной преступной группы.

Заместитель начальника К.Г. [illegible]



БСТМ
ГУ МВД России по г. Москве

Генеральному директору
ООО «Группа информационной безопасности»
И.К. Сачкову

Уважаемый Илья Константинович!

Бюро специальных технических мероприятий ГУ МВД России по г. Москве выражает благодарность экспертам Лаборатории компьютерной криминалистики и исследования вредоносного кода ООО "Группа информационной безопасности"

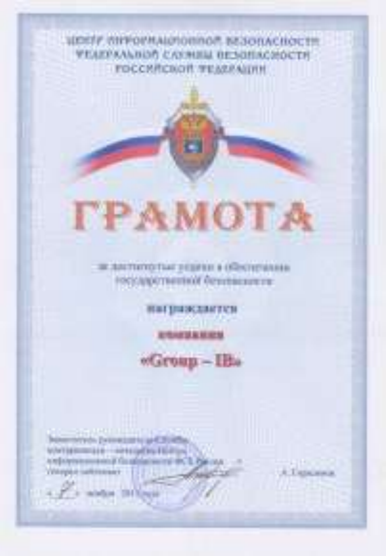
[illegible] Сергею Анатольевичу

[illegible] Александру Владимировичу

[illegible]

за экспертную поддержку по материалам, [illegible] сотрудниками БСТМ ГУ МВД России по г. Москве и активное участие при проведении мероприятий, следственных и иных действий.

Начальник К.Г. [illegible]



ЦЕНТР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ФЕДЕРАЛЬНОЙ СЛУЖБЫ БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ГРАМОТА

за достигнутые успехи в обеспечении
государственной безопасности

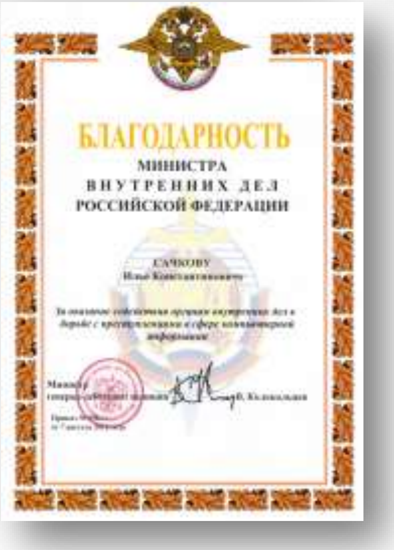
награждается

компания

«Group – IB»

Заместитель руководителя [illegible] Центра информационной безопасности ФСБ России [illegible] А. Герасимов

«[illegible]» ноября 201[illegible] года



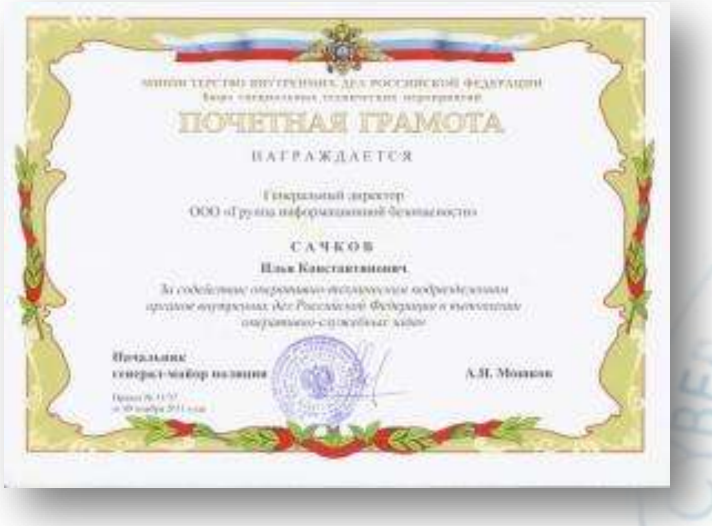
БЛАГОДАРНОСТЬ
МИНИСТРА
ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ

САЧКОВУ
Илье Константиновичу

За оказание содействия органам внутренних дел в борьбе с преступлениями в сфере компьютерной информации

Министр
генерал-лейтенант полиции В. Колокольцев

Приказ № [illegible]
от 7 августа 201[illegible] года



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
Бюро специальных технических мероприятий

ПОЧЕТНАЯ ГРАМОТА

НАГРАЖДАЕТСЯ

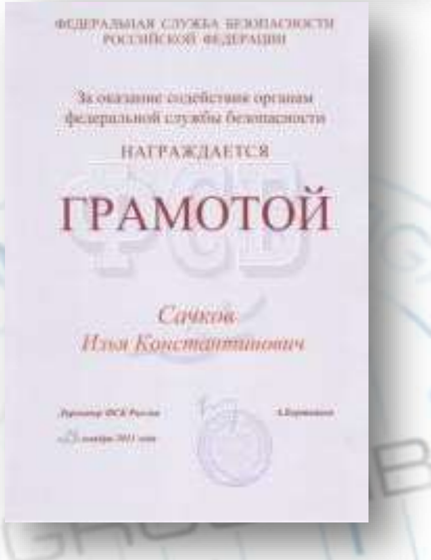
Генеральный директор
ООО «Группа информационной безопасности»

САЧКОВ
Илья Константинович

За содействие оперативно-техническим подразделениям органов внутренних дел Российской Федерации в выполнении оперативно-служебных задач

Начальник
генерал-майор полиции А.Н. Мошков

Приказ № 1137
от 30 ноября 2011 года



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

За оказание содействия органам
федеральной службы безопасности

НАГРАЖДАЕТСЯ

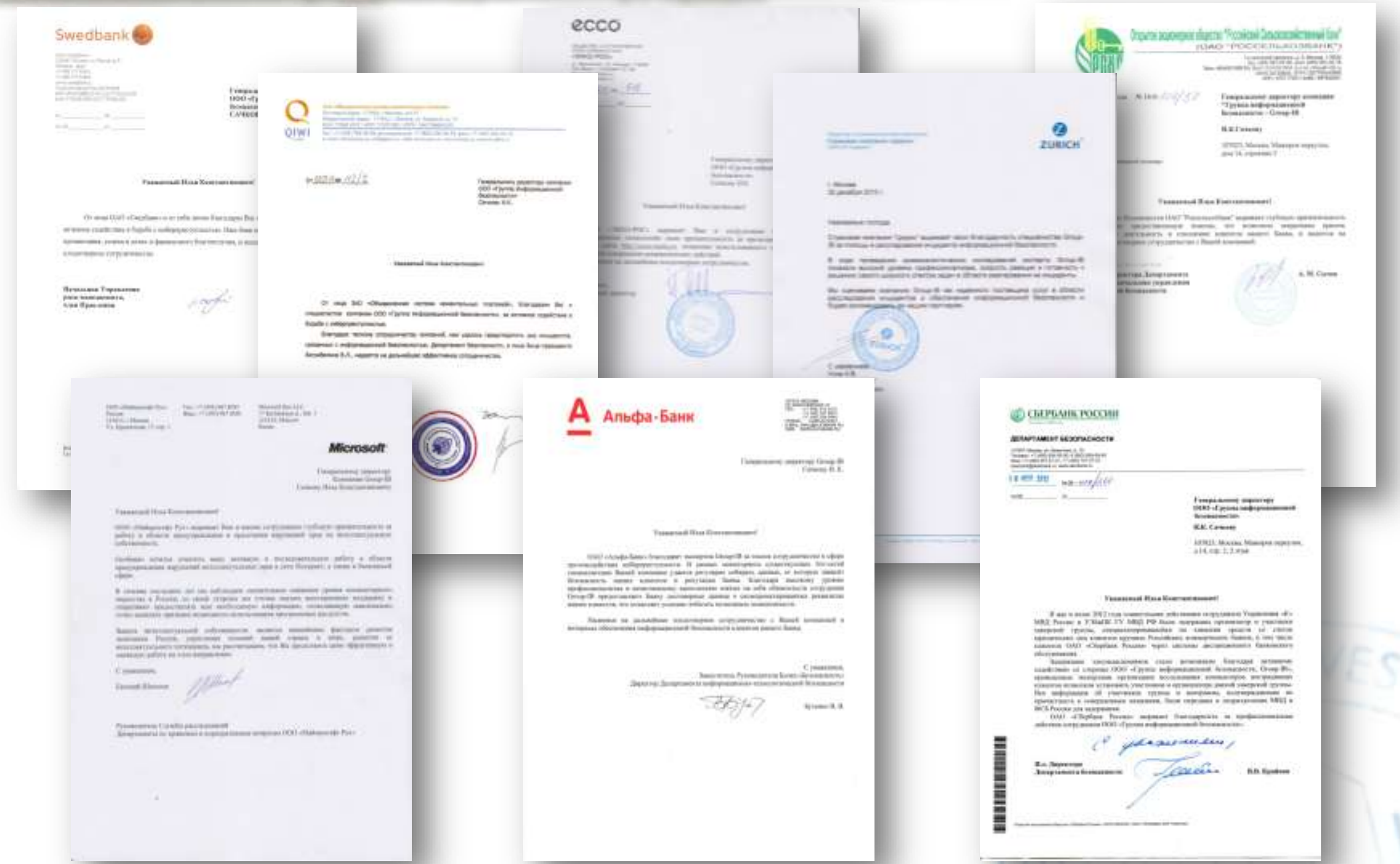
ГРАМОТОЙ

Сачков
Илья Константинович

Директор ФСБ России А.Бортников

«[illegible]» [illegible] 2011 года

References



Swedbank

QIWI

ecco

ZURICH

Открытое акционерное общество "Российский Сельскохозяйственный банк"
(ОАО "РОССЕЛЬХОЗБАНК")

Уважаемый Илья Константинович!

Microsoft

Альфа-Банк

Уважаемый Илья Константинович!

С уважением,

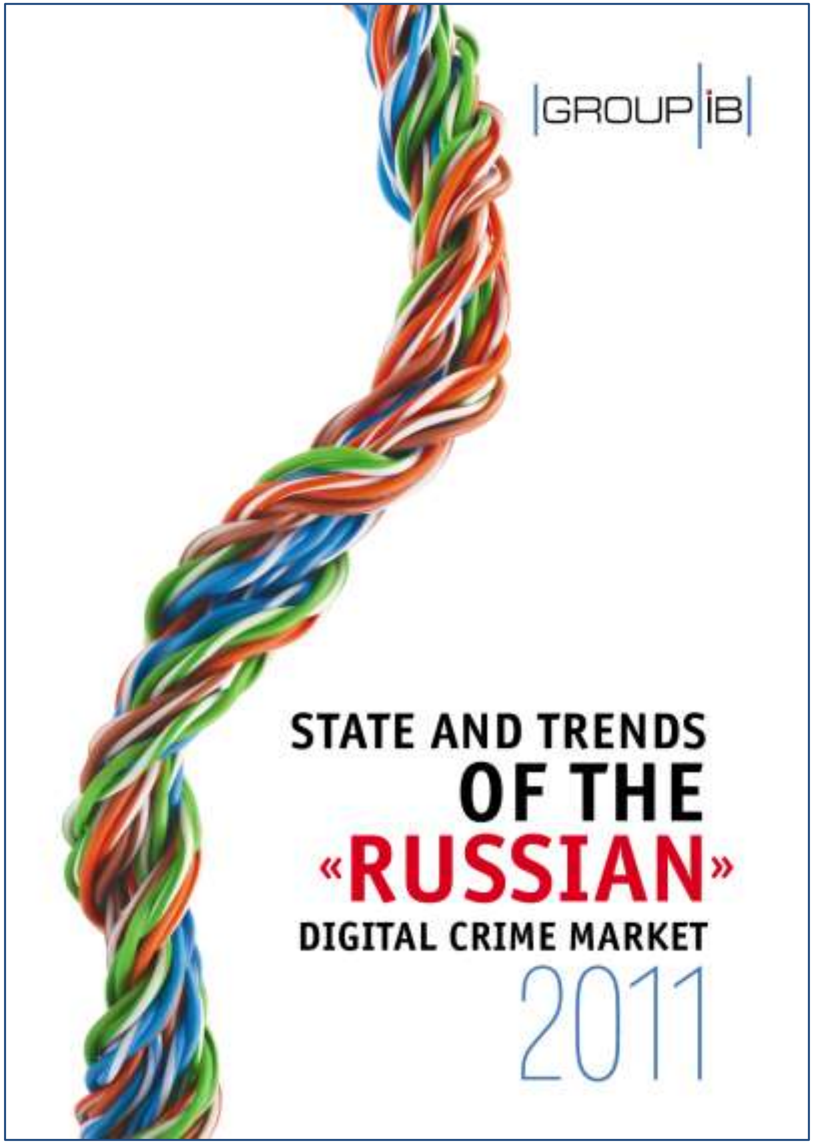
СБЕРБАНК РОССИИ

ДЕПАРТАМЕНТ БЕЗОПАСНОСТИ

Уважаемый Илья Константинович!

С уважением,

2011 Report



GROUP IB

STATE AND TRENDS OF THE «RUSSIAN» DIGITAL CRIME MARKET 2011

A report on the results of a comprehensive study of the state of the Russian-speaking cybercrime market:

- ✓ Financial performance estimates;
- ✓ Analysis of the main trends and threats;
- ✓ Overview of key events;
- ✓ Legal aspects;
- ✓ Forecasts.

Total Cybercrime Market

IN U.S. DOLLARS

RUSSIAN
CYBERCRIME MARKET

$2.3 billion

SIZE OF GLOBAL
CYBERCRIME MARKET

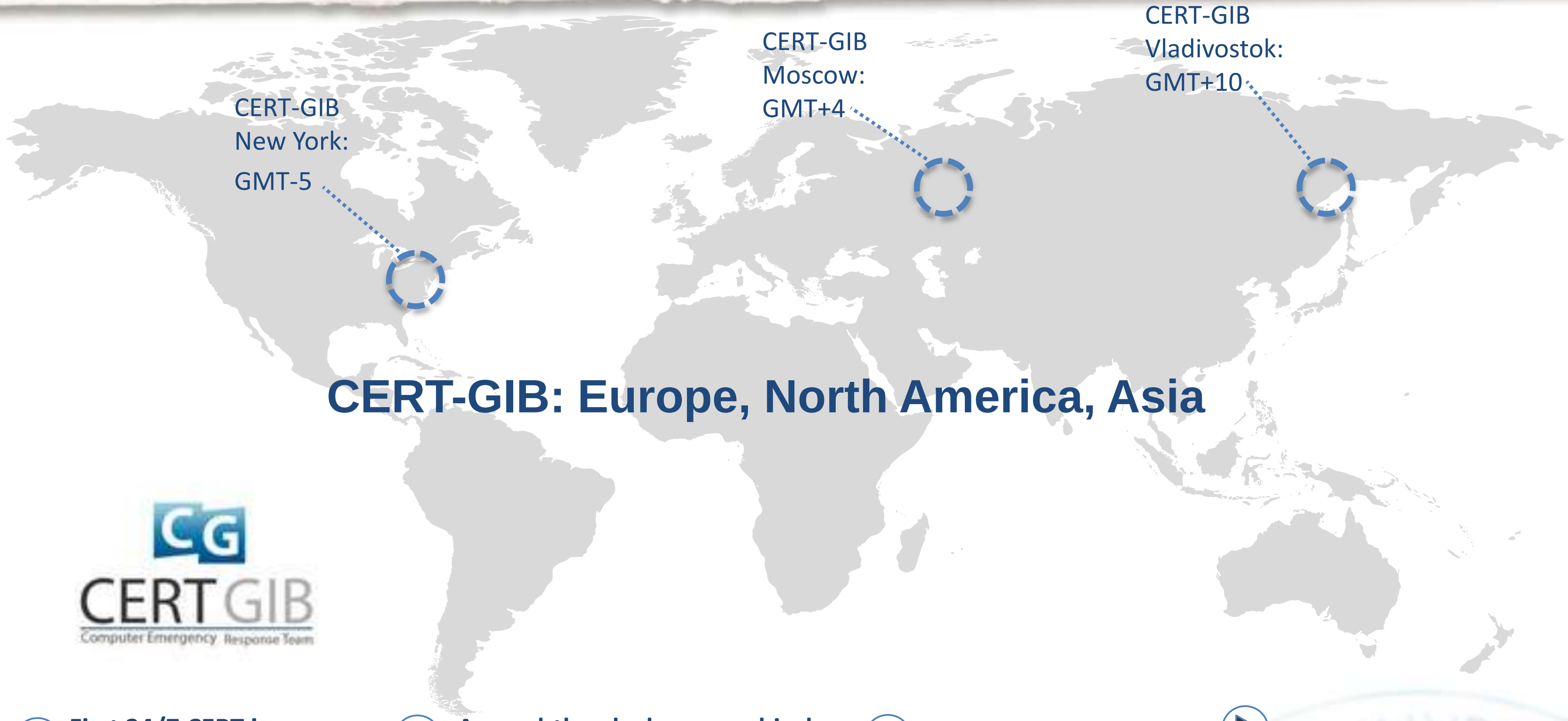
$12.5 billion

RUSSIAN SPEAKING
CYBERCRIME MARKET

$4.5 billion

Tot
er
rl
U.S
RUSSIAN
CYBERCRIME MARKET
$2.3 billion
RKET
.5
4.

CERT-GIB



CERT-GIB: Europe, North America, Asia

First 24/7 CERT in Eastern Europe

CERT-GIB is the first Eastern European 24/7 Computer Emergency Response Team, and the first private CERT in Russia (second overall)

Around-the-clock geographical deployent

Passing the relay for monitoring, analyzing, and mitigating:
Europe ➔ North America ➔ Asia
– for smooth uninterrupted incident handling

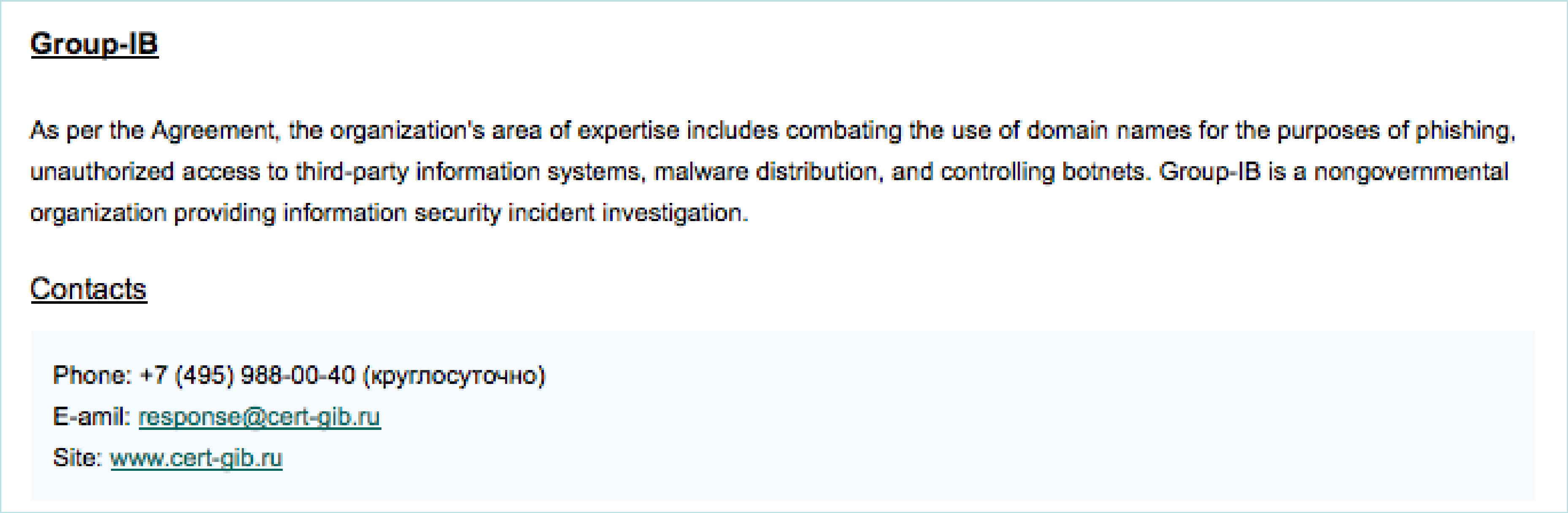
Providing help and assistance for:

Phishing, Spam, Scam, DDoS attacks, malware, and many other fraudulent schemes

.RU, .РФ, .SU: special emphasis

Official ccTLD.ru-assigned expert organization for handling phishing, malware, and botnets

CERT-GIB



Group-IB

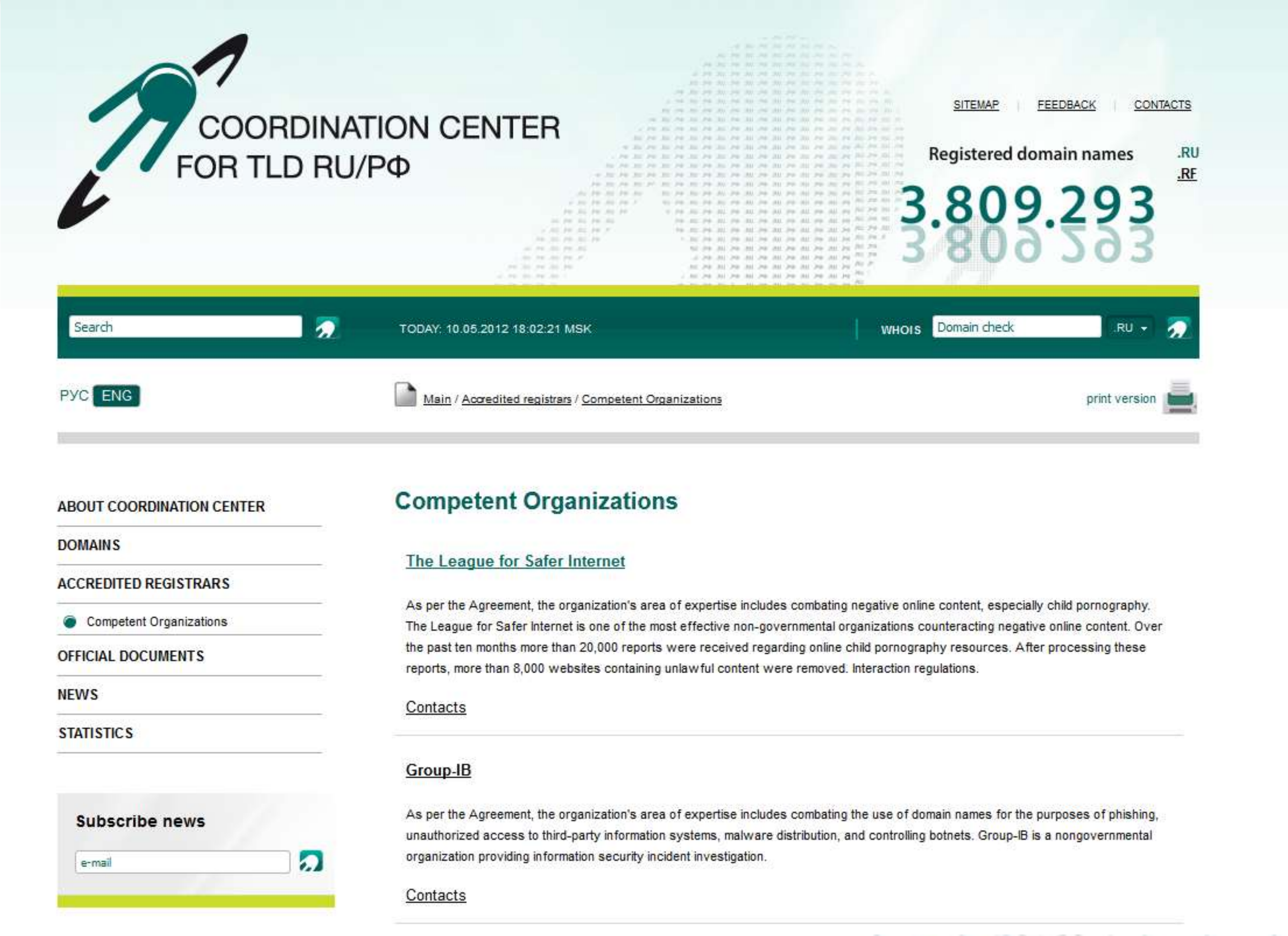
As per the Agreement, the organization's area of expertise includes combating the use of domain names for the purposes of phishing, unauthorized access to third-party information systems, malware distribution, and controlling botnets. Group-IB is a nongovernmental organization providing information security incident investigation.

Contacts

Phone: +7 (495) 988-00-40 (круглосуточно)
E-amil: response@cert-gib.ru
Site: www.cert-gib.ru

- Phishing
- Malware
- Botnets

Unique Expertise



COORDINATION CENTER
FOR TLD RU/РФ

Registered domain names .RU .RF

3.809.293

Main / Accredited registrars / Competent Organizations

Competent Organizations

The League for Safer Internet

As per the Agreement, the organization's area of expertise includes combating negative online content, especially child pornography. The League for Safer Internet is one of the most effective non-governmental organizations counteracting negative online content. Over the past ten months more than 20,000 reports were received regarding online child pornography resources. After processing these reports, more than 8,000 websites containing unlawful content were removed. Interaction regulations.

Contacts

Group-IB

As per the Agreement, the organization's area of expertise includes combating the use of domain names for the purposes of phishing, unauthorized access to third-party information systems, malware distribution, and controlling botnets. Group-IB is a nongovernmental organization providing information security incident investigation.

Contacts

CERT-GIB Accreditations

Authorized user of the "CERT" trademark

TI-listed team

Accreditation in progress

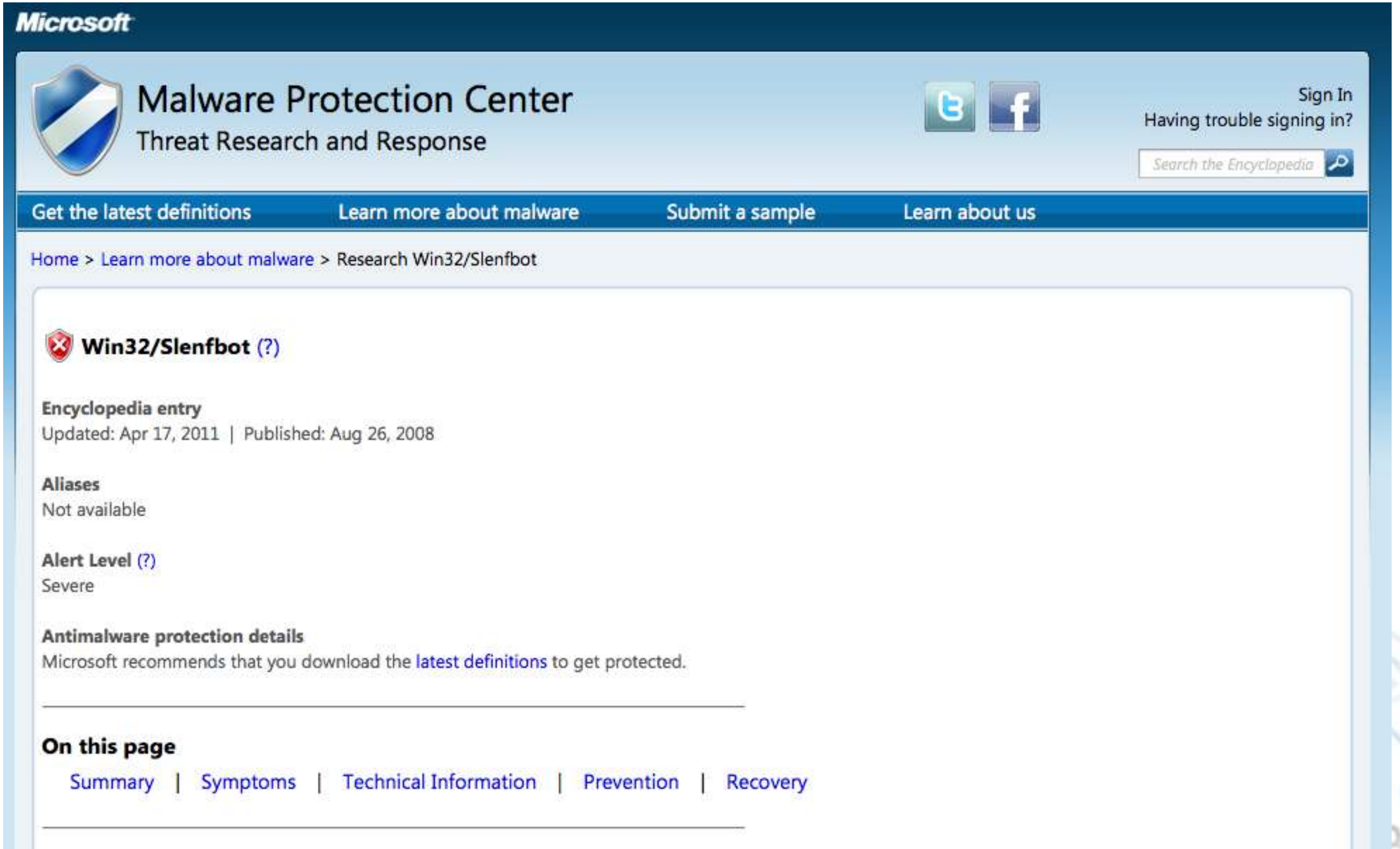
CERT-GIB Partners

- Microsoft
- Skype
- Symantec
- Abuse.ch
- Internet Identity
- Web of Trust
- Spamhaus

Methodology

1. Detect/get notified about a fraudulent domain
2. Analyze the information
3. Find substantial evidence
4. Form an abuse notification
5. Notify the registrar

Slenfbot: 600 000 users Skype, Yahoo, MSN



Microsoft
Malware Protection Center
Threat Research and Response
Sign In
Having trouble signing in?
Search the Encyclopedia
Get the latest definitions
Learn more about malware
Submit a sample
Learn about us

Home > Learn more about malware > Research Win32/Slenfbot

Win32/Slenfbot (?)

Encyclopedia entry
Updated: Apr 17, 2011 | Published: Aug 26, 2008

Aliases
Not available

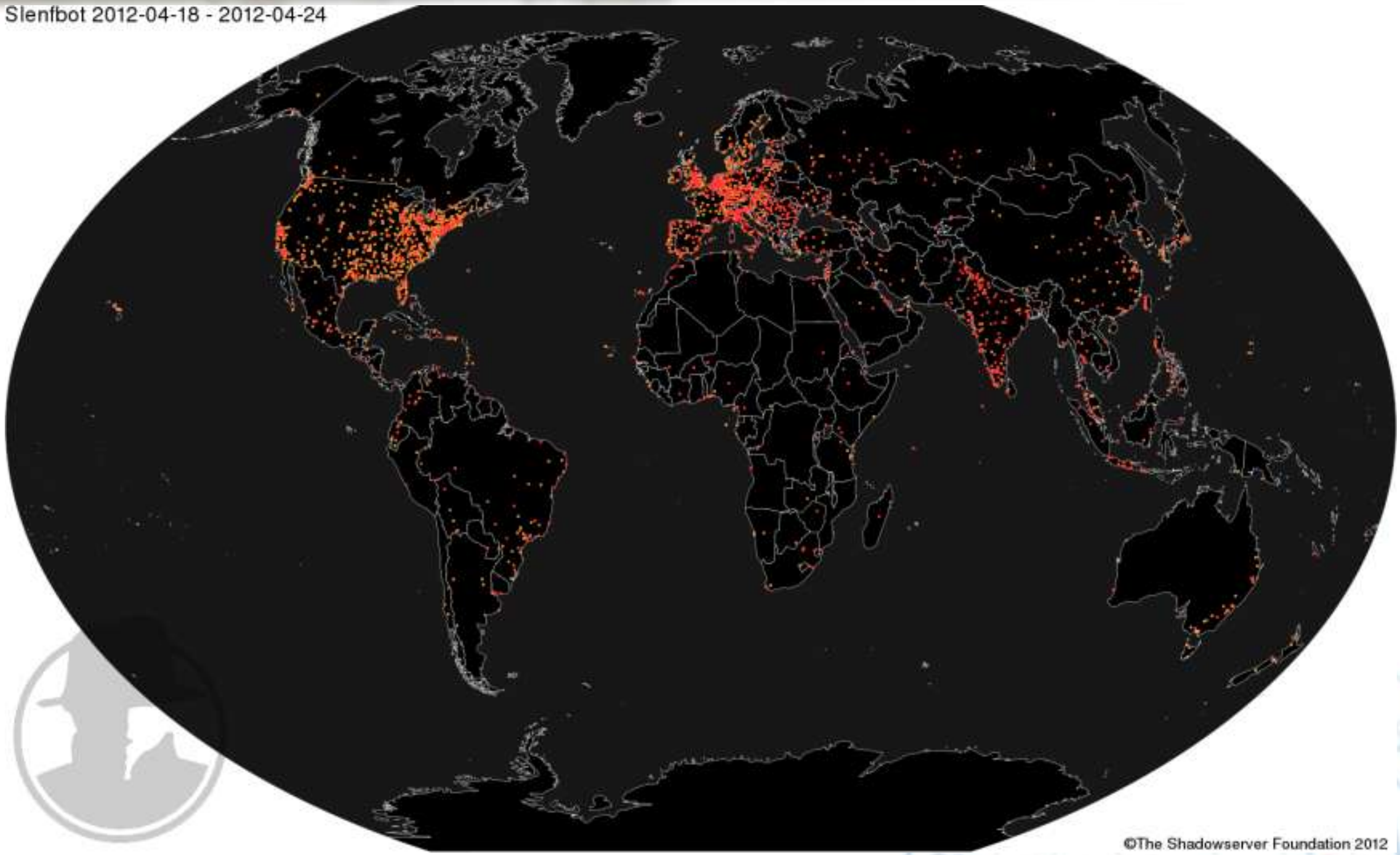
Alert Level (?)
Severe

Antimalware protection details
Microsoft recommends that you download the latest definitions to get protected.

On this page

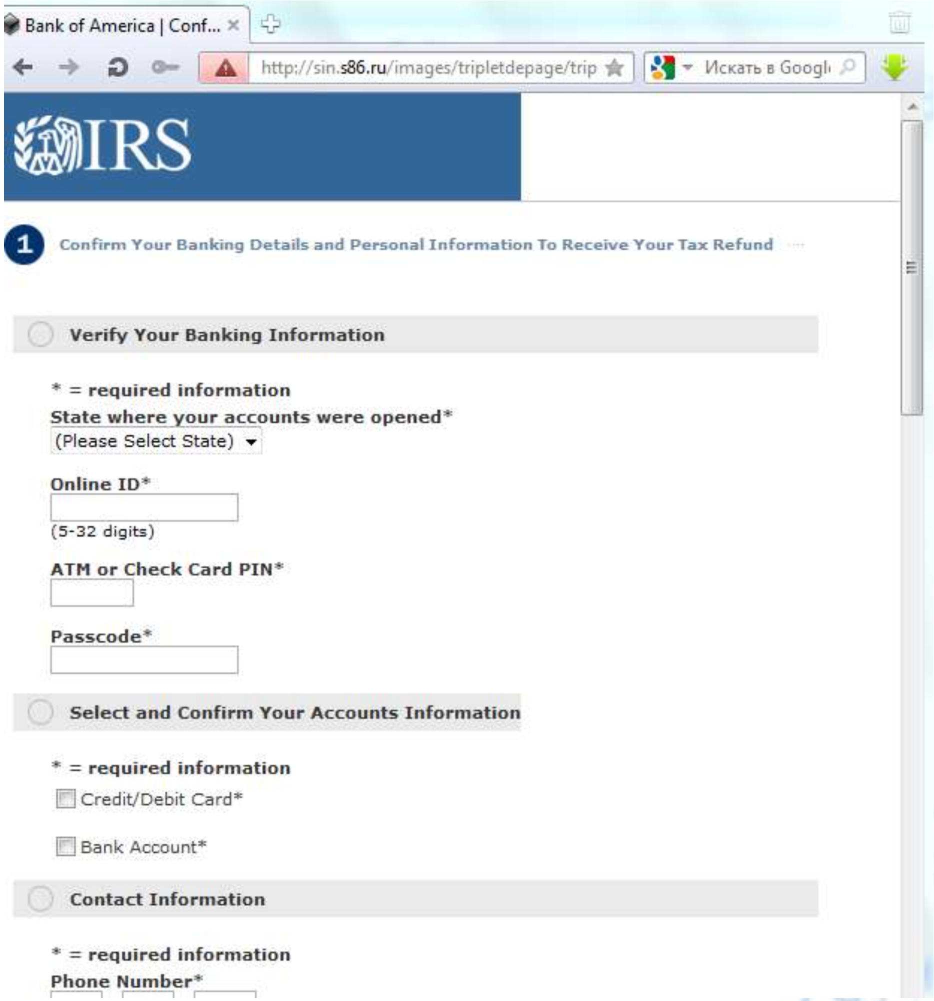
Summary | Symptoms | Technical Information | Prevention | Recovery

Slenfbot: 600 000 IP



©The Shadowserver Foundation 2012

Phishing on a compromised host


Bank of America | Conf...
http://sin.s86.ru/images/tripletdepage/trip
Искать в Googl
IRS

1 Confirm Your Banking Details and Personal Information To Receive Your Tax Refund

○ **Verify Your Banking Information**

* = required information

State where your accounts were opened*

(Please Select State) ▾

Online ID*

(5-32 digits)

ATM or Check Card PIN*

Passcode*

○ **Select and Confirm Your Accounts Information**

* = required information

□ Credit/Debit Card*

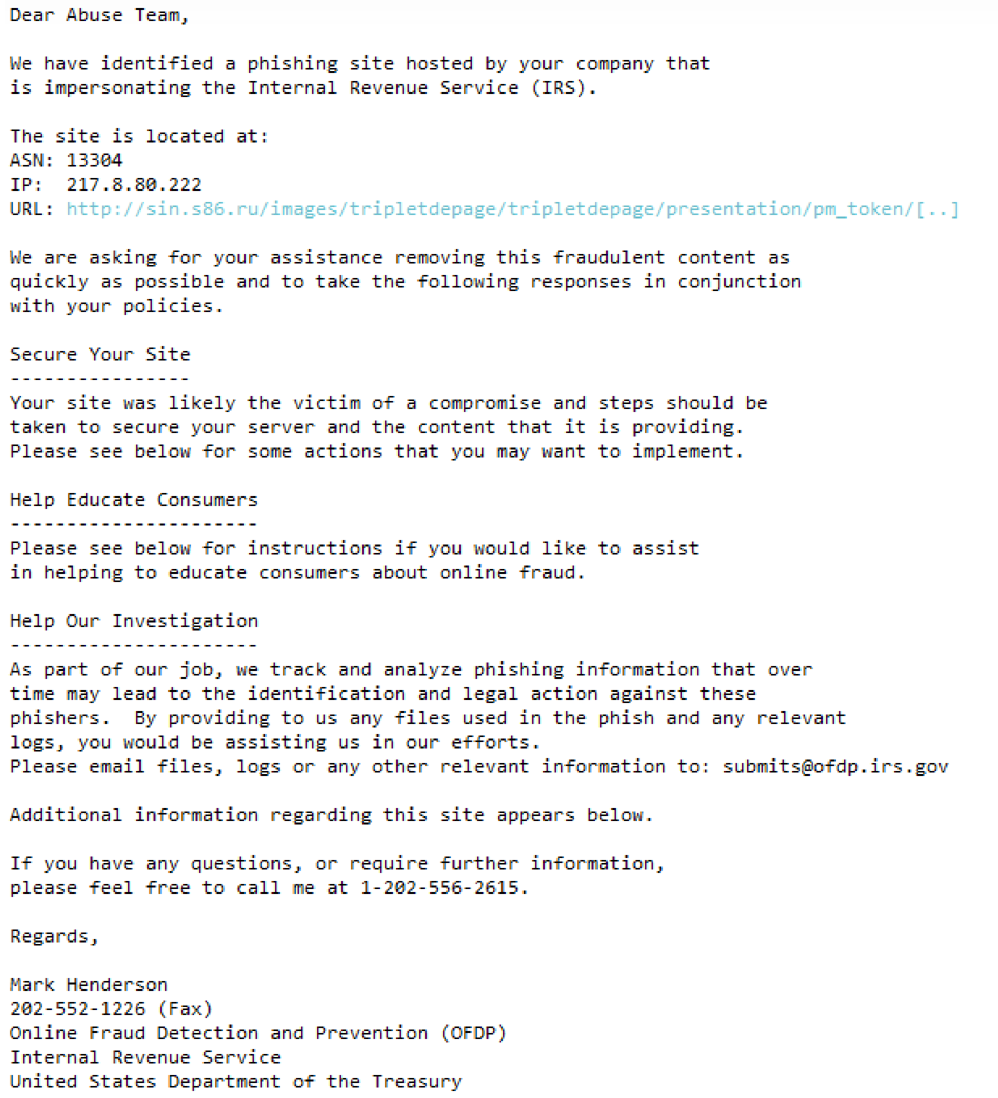
□ Bank Account*

○ **Contact Information**

* = required information

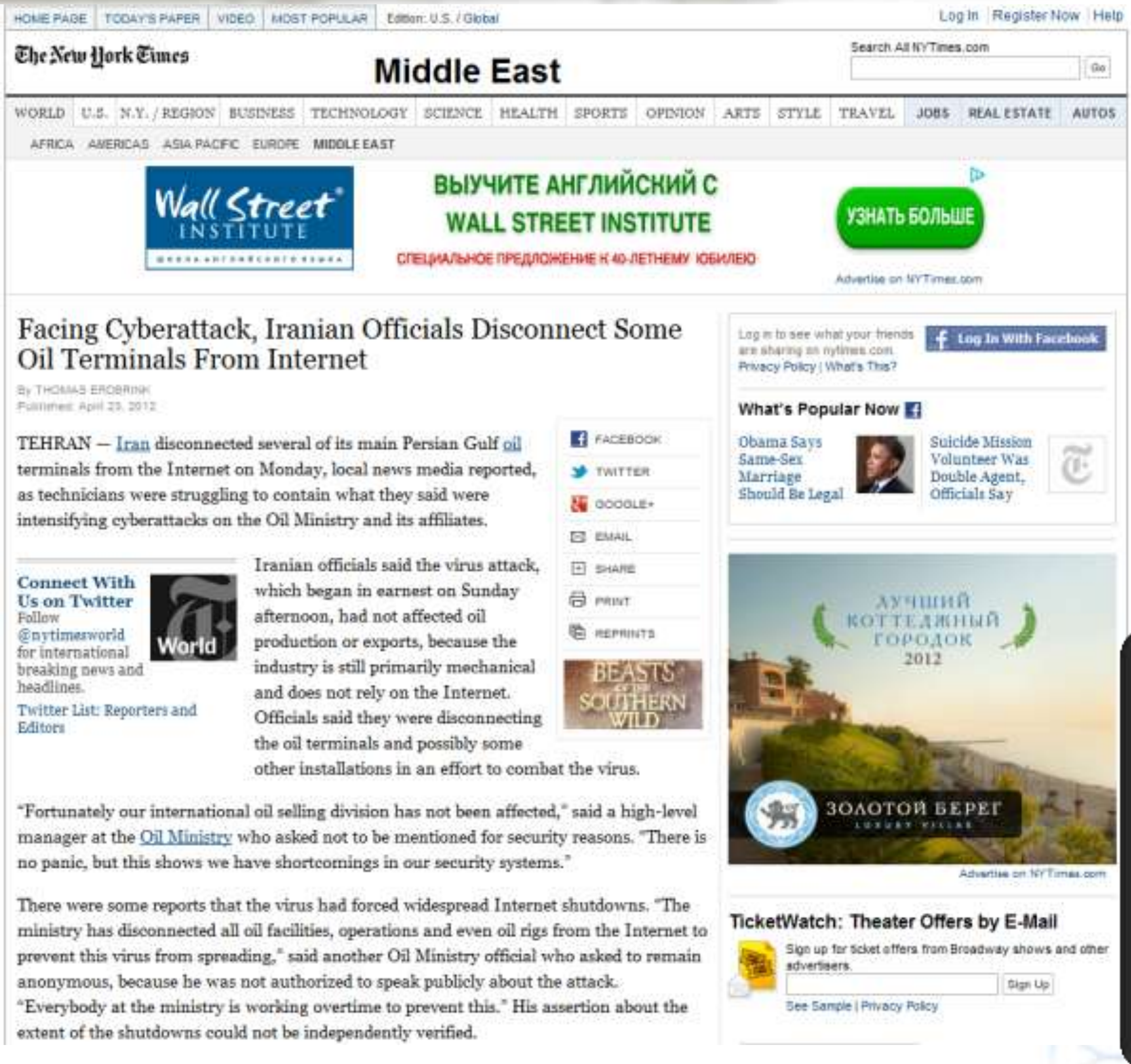
Phone Number*

Phishing on a compromised host



```
Dear Abuse Team,

We have identified a phishing site hosted by your company that
is impersonating the Internal Revenue Service (IRS).

The site is located at:
ASN: 13304
IP:  217.8.80.222
URL: http://sin.s86.ru/images/tripletdepage/tripletdepage/presentation/pm_token/[..]

We are asking for your assistance removing this fraudulent content as
quickly as possible and to take the following responses in conjunction
with your policies.

Secure Your Site
----------------
Your site was likely the victim of a compromise and steps should be
taken to secure your server and the content that it is providing.
Please see below for some actions that you may want to implement.

Help Educate Consumers
----------------------
Please see below for instructions if you would like to assist
in helping to educate consumers about online fraud.

Help Our Investigation
----------------------
As part of our job, we track and analyze phishing information that over
time may lead to the identification and legal action against these
phishers.  By providing to us any files used in the phish and any relevant
logs, you would be assisting us in our efforts.
Please email files, logs or any other relevant information to: submits@ofdp.irs.gov

Additional information regarding this site appears below.

If you have any questions, or require further information,
please feel free to call me at 1-202-556-2615.

Regards,

Mark Henderson
202-552-1226 (Fax)
Online Fraud Detection and Prevention (OFDP)
Internal Revenue Service
United States Department of the Treasury
```

Cyber attack on Iranian pipelines



HOME PAGE | TODAY'S PAPER | VIDEO | MOST POPULAR | Edition: U.S. / Global

Log In | Register Now | Help

The New York Times

Middle East

Search All NYTimes.com

Go

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION | ARTS | STYLE | TRAVEL | JOBS | REAL ESTATE | AUTOS

AFRICA | AMERICAS | ASIA PACIFIC | EUROPE | MIDDLE EAST

Facing Cyberattack, Iranian Officials Disconnect Some Oil Terminals From Internet

By THOMAS ERDBRINK
Published: April 23, 2012

TEHRAN — Iran disconnected several of its main Persian Gulf oil terminals from the Internet on Monday, local news media reported, as technicians were struggling to contain what they said were intensifying cyberattacks on the Oil Ministry and its affiliates.

Iranian officials said the virus attack, which began in earnest on Sunday afternoon, had not affected oil production or exports, because the industry is still primarily mechanical and does not rely on the Internet. Officials said they were disconnecting the oil terminals and possibly some other installations in an effort to combat the virus.

"Fortunately our international oil selling division has not been affected," said a high-level manager at the Oil Ministry who asked not to be mentioned for security reasons. "There is no panic, but this shows we have shortcomings in our security systems."

There were some reports that the virus had forced widespread Internet shutdowns. "The ministry has disconnected all oil facilities, operations and even oil rigs from the Internet to prevent this virus from spreading," said another Oil Ministry official who asked to remain anonymous, because he was not authorized to speak publicly about the attack. "Everybody at the ministry is working overtime to prevent this." His assertion about the extent of the shutdowns could not be independently verified.

Connect With Us on Twitter
Follow @nytimesworld for international breaking news and headlines.
Twitter List: Reporters and Editors

World

FACEBOOK
TWITTER
GOOGLE+
EMAIL
SHARE
PRINT
REPRINTS

Log in to see what your friends are sharing on nytimes.com.
Privacy Policy | What's This?

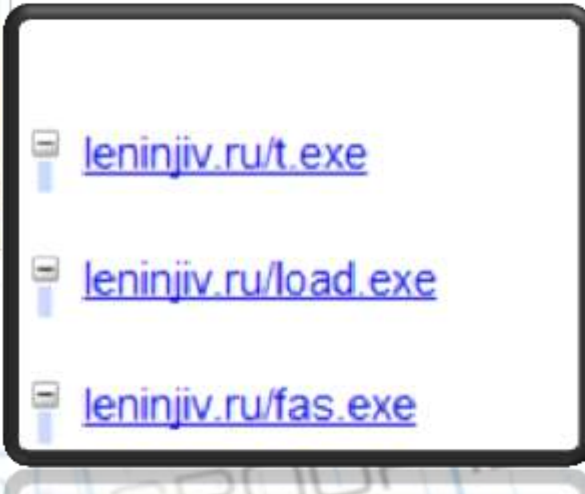
Log In With Facebook

What's Popular Now

Obama Says Same-Sex Marriage Should Be Legal

Suicide Mission Volunteer Was Double Agent, Officials Say

TicketWatch: Theater Offers by E-Mail
Sign up for ticket offers from Broadway shows and other advertisers.
Sign Up
See Sample | Privacy Policy



leninjiv.ru/t.exe

leninjiv.ru/load.exe

leninjiv.ru/fas.exe

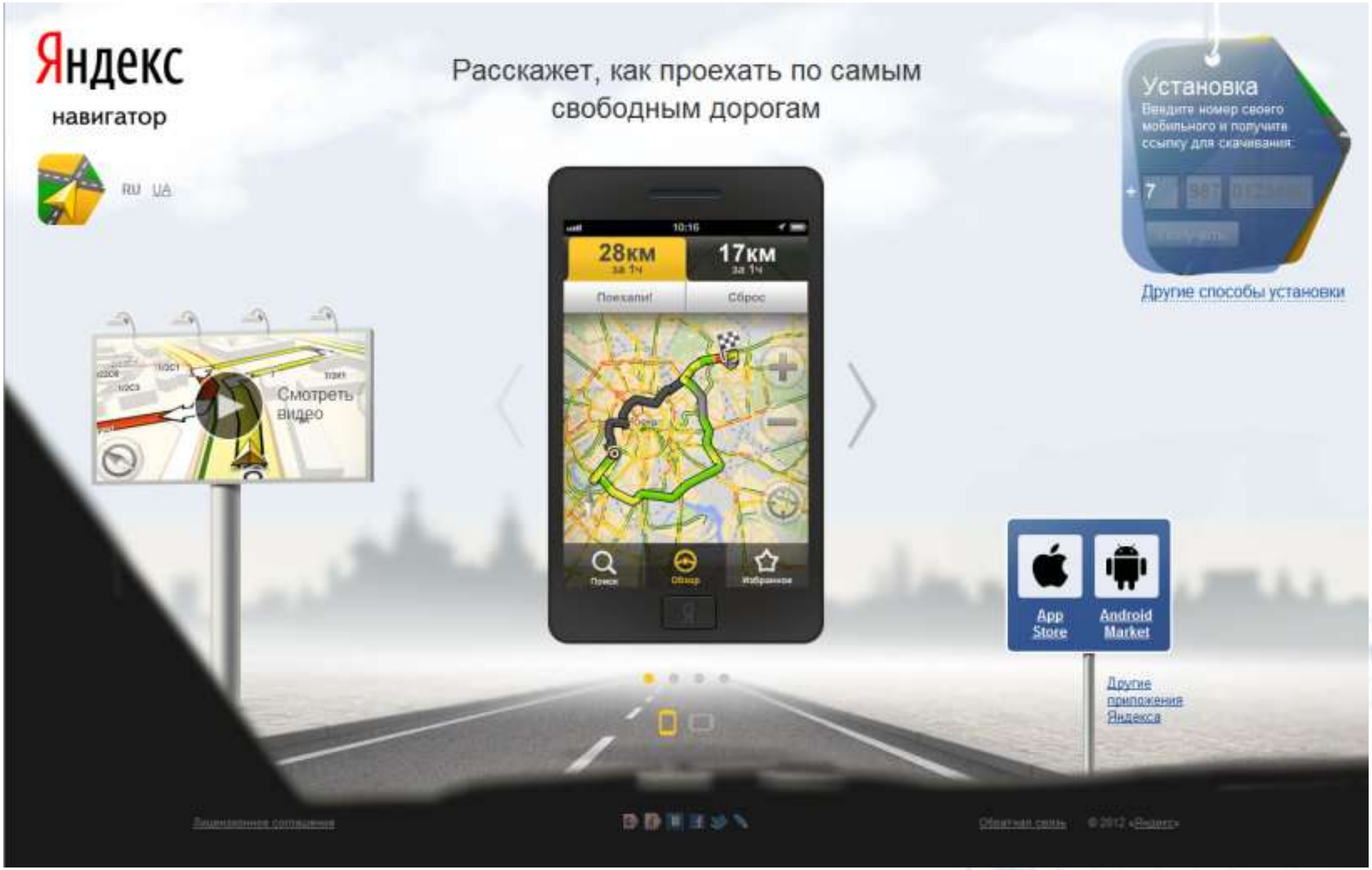
http://www.nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html

Cyber attack on Iranian pipelines

REAL PROGRESS

```
domain:        LENINJIV.RU
nserver:       ns1.usahosting2012.com.
nserver:       ns2.usahosting2012.com.
nserver:       ns3.usahosting2012.com.
nserver:       ns4.usahosting2012.com.
state:        REGISTERED, NOT DELEGATED,
UNVERIFIED
person:        Private Person
registrar:     NAUNET-REG-RIPN
admin-contact:
https://client.naunet.ru/c/whoiscontact
created:       2012.04.28
paid-till:     2013.04.28
free-date:     2013.05.29
source:        TCI
```

Yandex-navigator.ru



Яндекс навигатор

Расскажет, как проехать по самым свободным дорогам

Установка

Введите номер своего мобильного и получите ссылку для скачивания:

Другие способы установки

Другие приложения Яндекса

Лицензионное соглашение

Обратная связь © 2012 «Яндекс»

Yandex-navigator.ru

```
GET /skript/reklama.php HTTP/1.1
Host: yandex-navigator.ru
User-Agent: Opera/9.30 (Nintendo Wii; U; ; 2047-7; en)
Accept: */*
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://yandex-navigator.ru/
HTTP/1.1 200 OK
Date: Tue, 17 Apr 2012 20:25:33 GMT
Server: Apache/2.0.63 (FreeBSD) PHP/5.2.12 with Suhosin-Patch
X-Powered-By: PHP/5.2.12
--------------------------------------------------------
GET /d.php?a=t294x294w215x2w4u2w423m254l2u266r213640384x2c4w2c443&nb&id=40 HTTP/1.1
Host: iplay-android.net
User-Agent: Opera/9.30 (Nintendo Wii; U; ; 2047-7; en)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://iplay-android.net/detail.php?a=t294x294w215x2w4u2w423m254l2u266r213640384x2c4w2c443&nb&id=40&auto=2
Cookie: PHPSESSID=vgrsp5g4guifgqfrgot954cf95; lvisit=15881-74; ldownload=15881-74

HTTP/1.1 302 Found
Server: nginx/1.0.9
Set-Cookie: ldownload=15881-74; expires=Wed, 18-Apr-2012 20:56:04 GMT
Location: http://failii.ru/midlets/15881_302817985/.apk
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 20
--------------------------------------------------------
http://failii.ru/midlets/15881_302817985/.apk
```

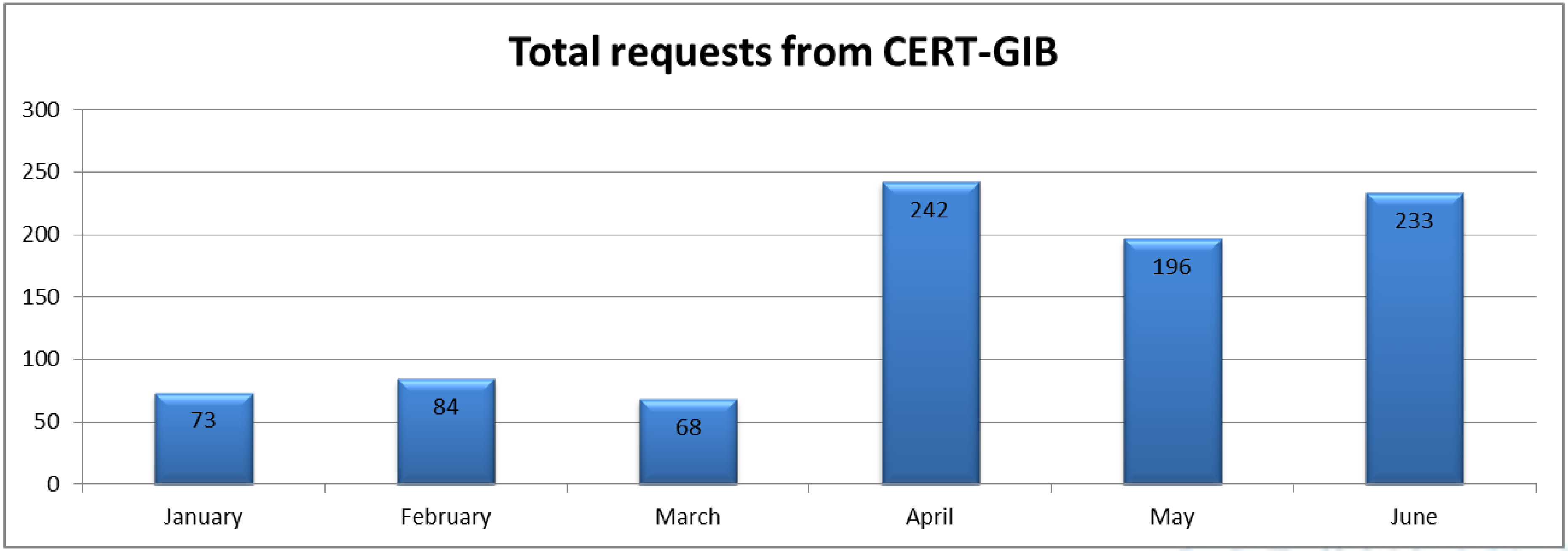
Results of the Investigation

- ✓ Joint investigation in close cooperation with the **FSB** and **MVD** of the Russian Federation and **FOX-IT**;
- ✓ Results of the investigation is the detention of the criminal group (8 persons);
- ✓ World’s first case when the entire online-banking criminal chain was arrested.

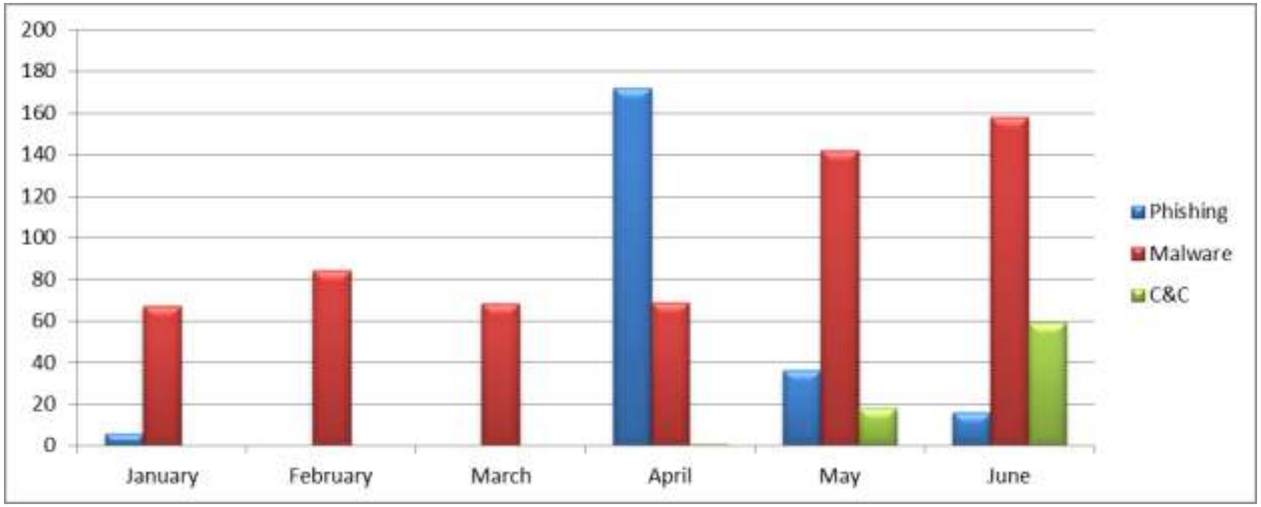
Conclusion

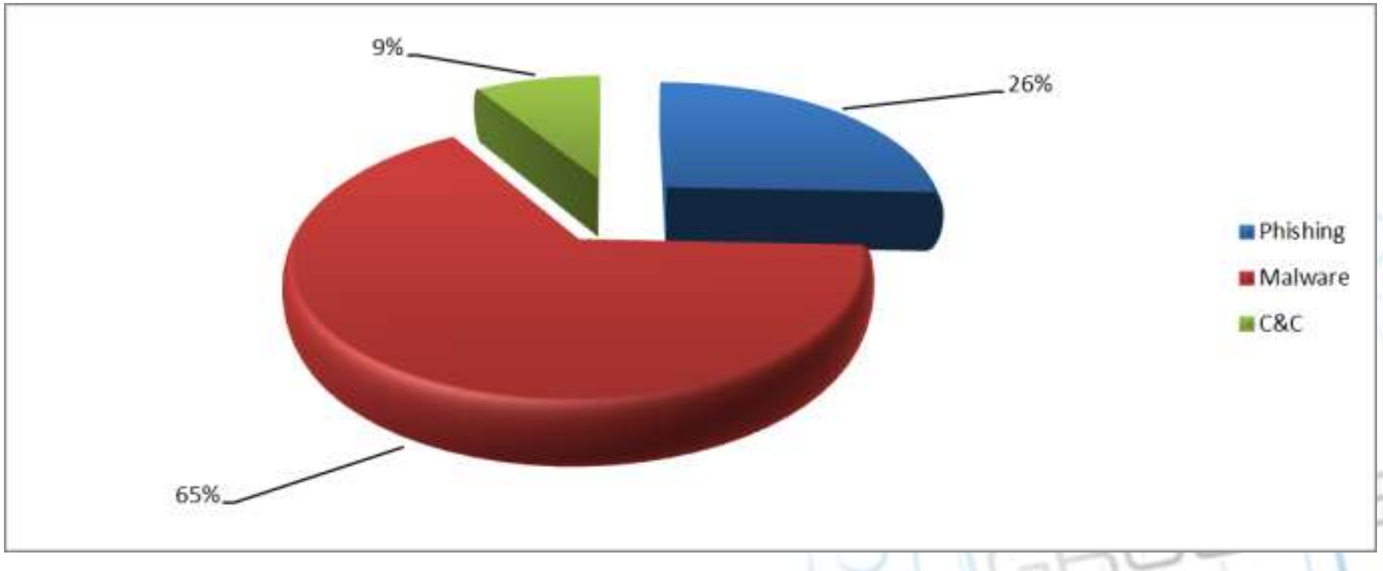
- ✓Three of six active groups arrested;
- ✓Remaining 3 groups are under investigation;
- ✓Law enforcement officials are becoming more interested in such crimes;
- ✓With proper support, at least three criminal groups can be neutralized within eight months;
- ✓We expect a surge in theft, including from individuals, in June and July 2012.

Total requests



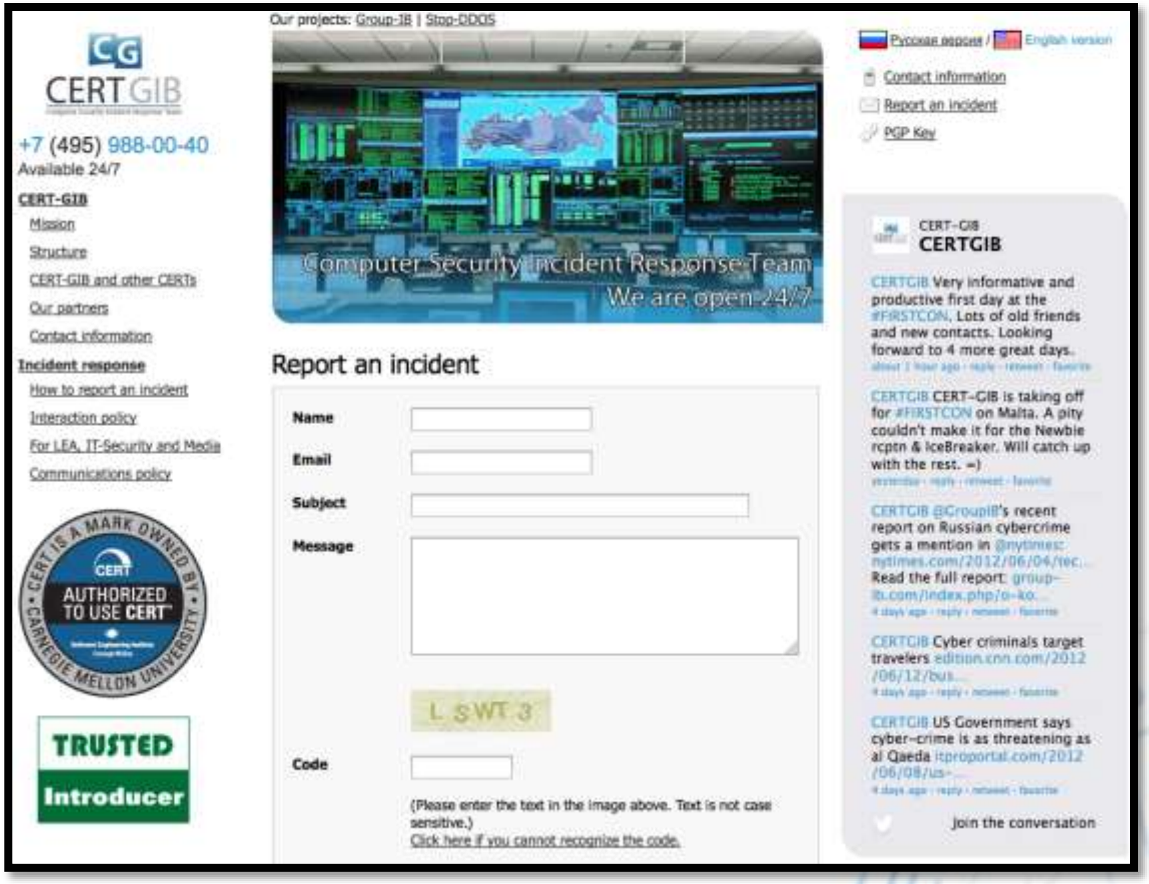
Types of threats





Ways to submit badness

response@cert-gib.ru



Our projects: Group-IB | Stop-DDOS

CERT GIB

+7 (495) 988-00-40
Available 24/7

CERT-GIB

- Mission
- Structure
- CERT-GIB and other CERTs
- Our partners
- Contact information

Incident response

- How to report an incident
- Interaction policy
- For LEA, IT-Security and Media
- Communications policy

CERT IS A MARK OWNED BY CARNEGIE MELLON UNIVERSITY · CERT AUTHORIZED TO USE CERT™

TRUSTED Introducer

Computer Security Incident Response Team
We are open 24/7

Report an incident

Name	
Email	
Subject	
Message	
	L SWT 3
Code	

(Please enter the text in the image above. Text is not case sensitive.)
Click here if you cannot recognize the code.

Русская версия / English version

- Contact information
- Report an incident
- PGP Key

CERT-GIB
CERTGIB

CERTGIB Very informative and productive first day at the #FIRSTCON. Lots of old friends and new contacts. Looking forward to 4 more great days.
about 1 hour ago · reply · retweet · favorite

CERTGIB CERT-GIB is taking off for #FIRSTCON on Malta. A pity couldn't make it for the Newbie rcptn & IceBreaker. Will catch up with the rest. =)
yesterday · reply · retweet · favorite

CERTGIB @GroupIB's recent report on Russian cybercrime gets a mention in @nytimes: nytimes.com/2012/06/04/tec... Read the full report: group-ib.com/index.php/o-ko...
4 days ago · reply · retweet · favorite

CERTGIB Cyber criminals target travelers edition.cnn.com/2012/06/12/bus...
4 days ago · reply · retweet · favorite

CERTGIB US Government says cyber-crime is as threatening as al Qaeda itproportal.com/2012/06/08/us-...
4 days ago · reply · retweet · favorite

Join the conversation

Group-IB

Ilya Sachkov

CEO

+7 (495) 661-55-38
sachkov@group-ib.com
www.group-ib.com

CYBER CRIMES INVESTIGATION • CYBER CRIMES INVESTIGATION •

GROUP IB

+7 495 661 55 38 www.group-ib.com www.letagroup.ru