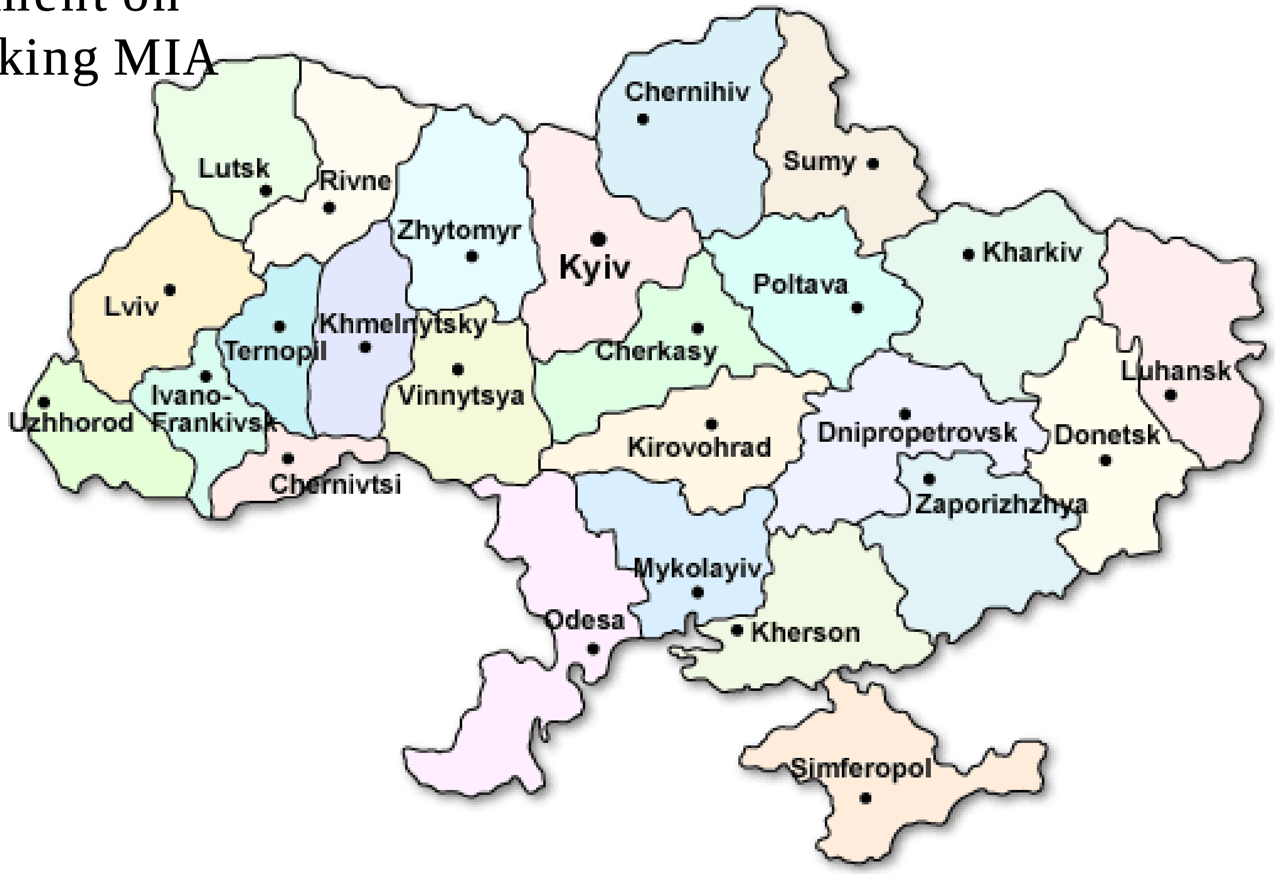
УПРАВЛІННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ
@ МВС УКРАЇНИ @

Ministry of Internal Affairs

Department on combating cybercrimes

Cybercrime Division started in 2009 as a unit in Department on combating human trafficking MIA of Ukraine

In 2011 a separate Department was created



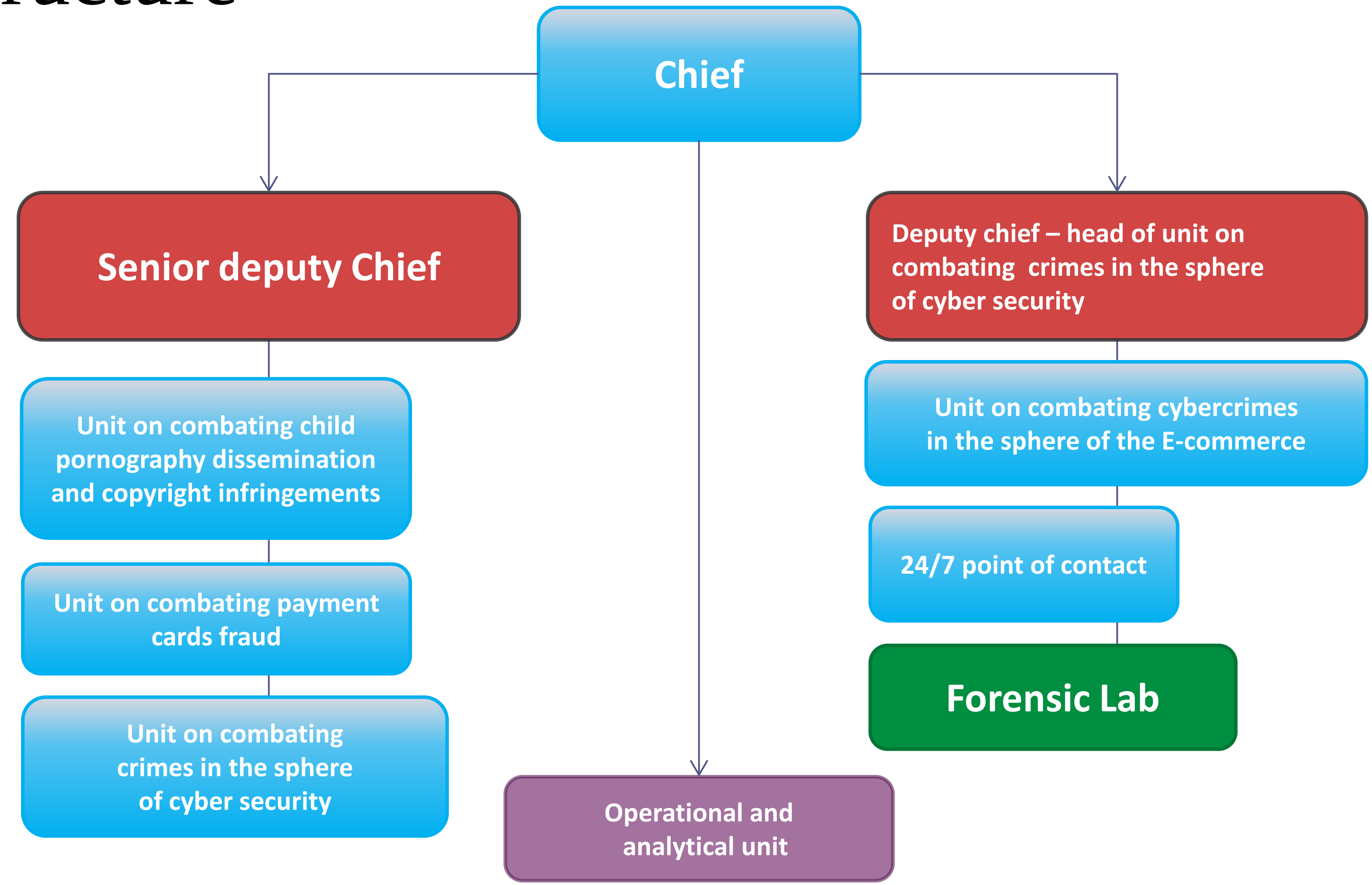
Headquarter is located in Kiev (33 agents)

25 regional divisions in each region (256 agents)

24/7 response center

Forensic lab

Structure



Chief

Senior deputy Chief

Unit on combating child pornography dissemination and copyright infringements

Unit on combating payment cards fraud

Unit on combating crimes in the sphere of cyber security

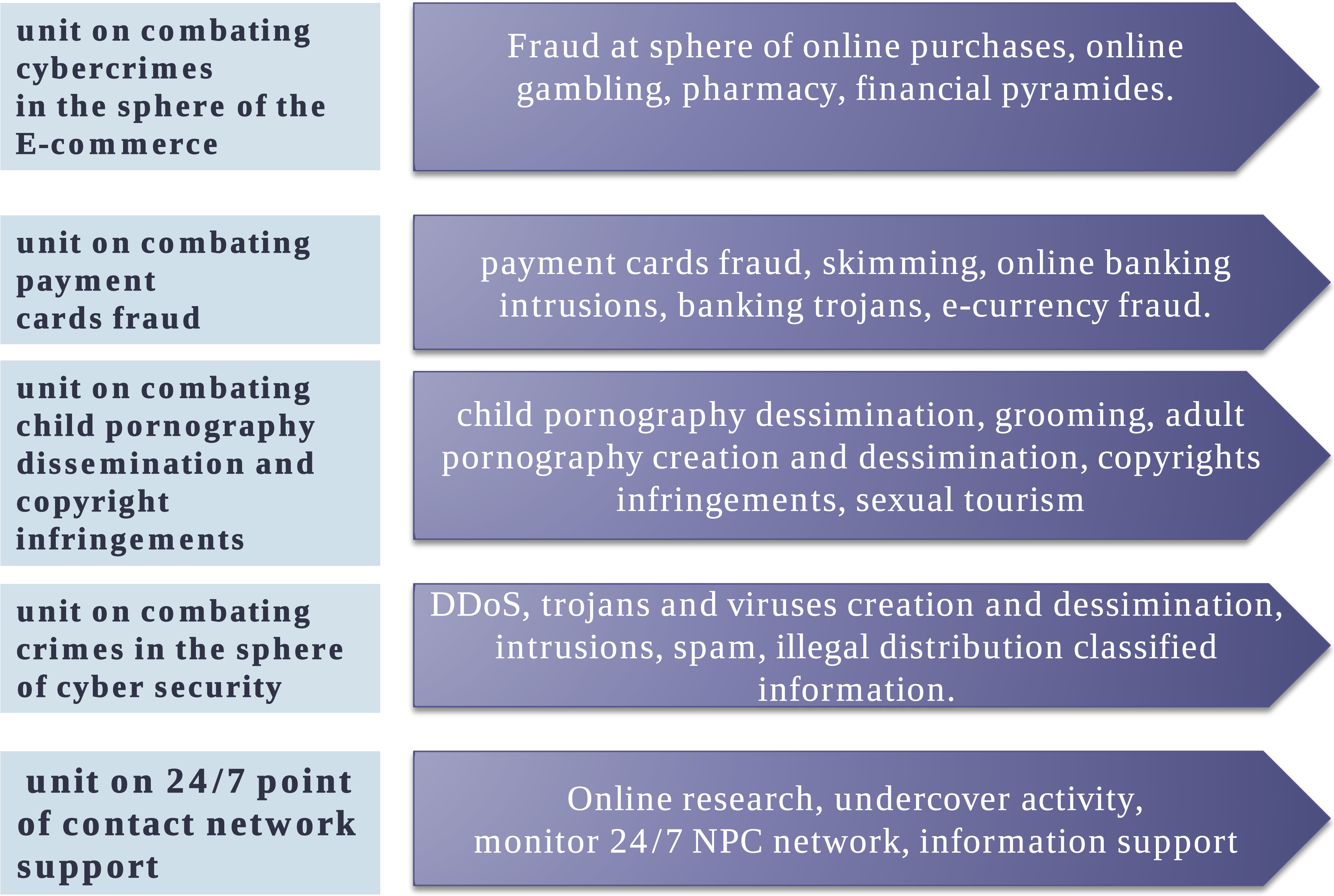
Operational and analytical unit

Deputy chief – head of unit on combating crimes in the sphere of cyber security

Unit on combating cybercrimes in the sphere of the E-commerce

24/7 point of contact

Forensic Lab



unit on combating cybercrimes in the sphere of the E-commerce	Fraud at sphere of online purchases, online gambling, pharmacy, financial pyramides.
unit on combating payment cards fraud	payment cards fraud, skimming, online banking intrusions, banking trojans, e-currency fraud.
unit on combating child pornography dissemination and copyright infringements	child pornography dessimination, grooming, adult pornography creation and dessimination, copyrights infringements, sexual tourism
unit on combating crimes in the sphere of cyber security	DDoS, trojans and viruses creation and dessimination, intrusions, spam, illegal distribution classified information.
unit on 24/7 point of contact network support	Online research, undercover activity, monitor 24/7 NPC network, information support

Forensic lab

Created with support of US Embassy in Ukraine.

The main aims are:

- forensic examination of seized evidence;
- supporting agents in the investigations;
- collecting evidences;

Training center:

Conducting trainings for the agents, investigators and prosecutors

24/7

According to the article 35 Convention on Cybercrime, in Department on combating cybercrimes was created **27/7 contact point.**

Functions:

- the provision of technical advice;

- the preservation of data;

- the collection of evidence, the provision of legal information, and locating of suspects.

Contacts:
email:request@cybercrime.gov.ua,
tel: +380443743777

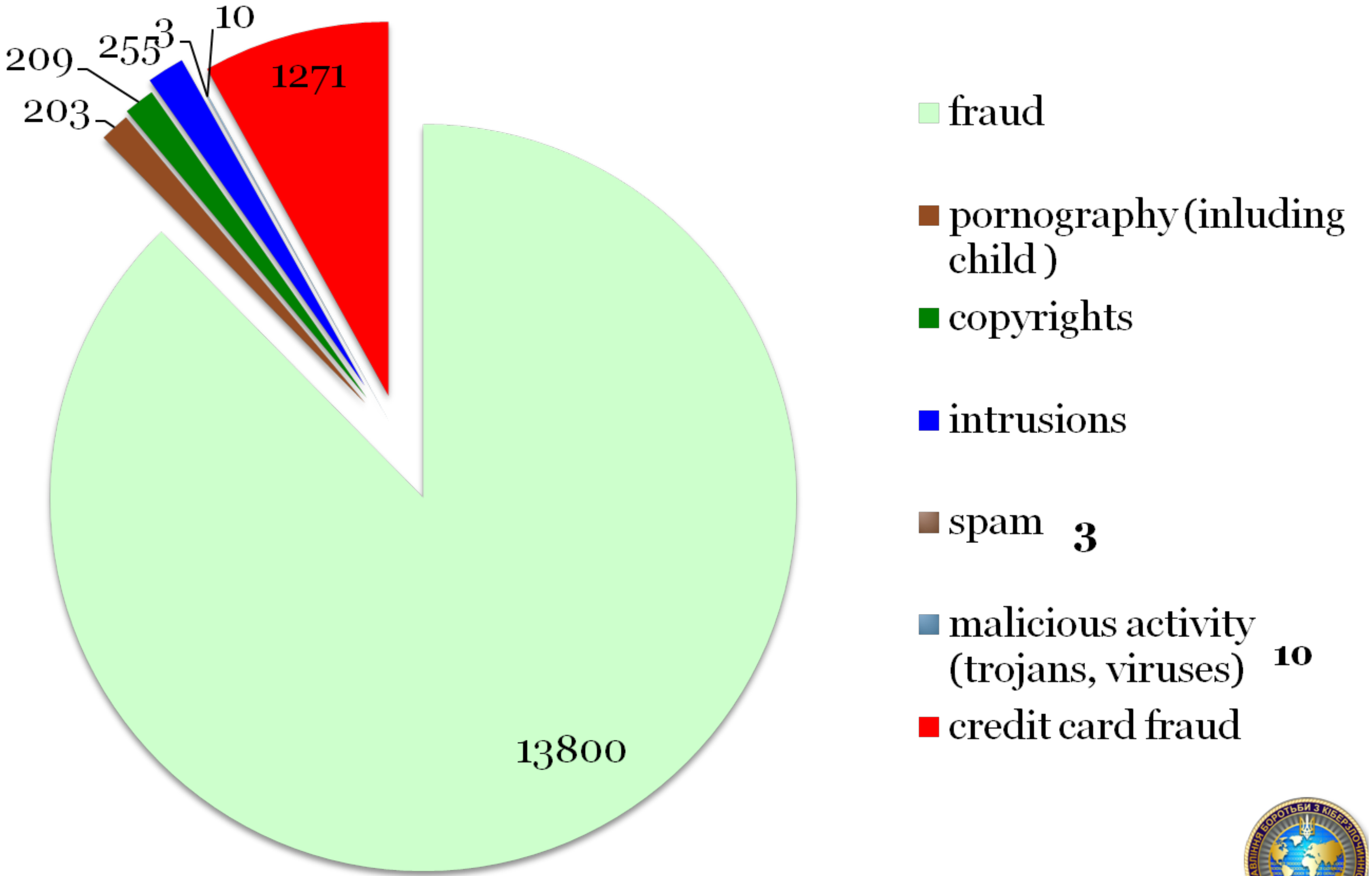
Our competence

According to art. 216 Criminal-procedure code of Ukraine police is able to investigate cases about:

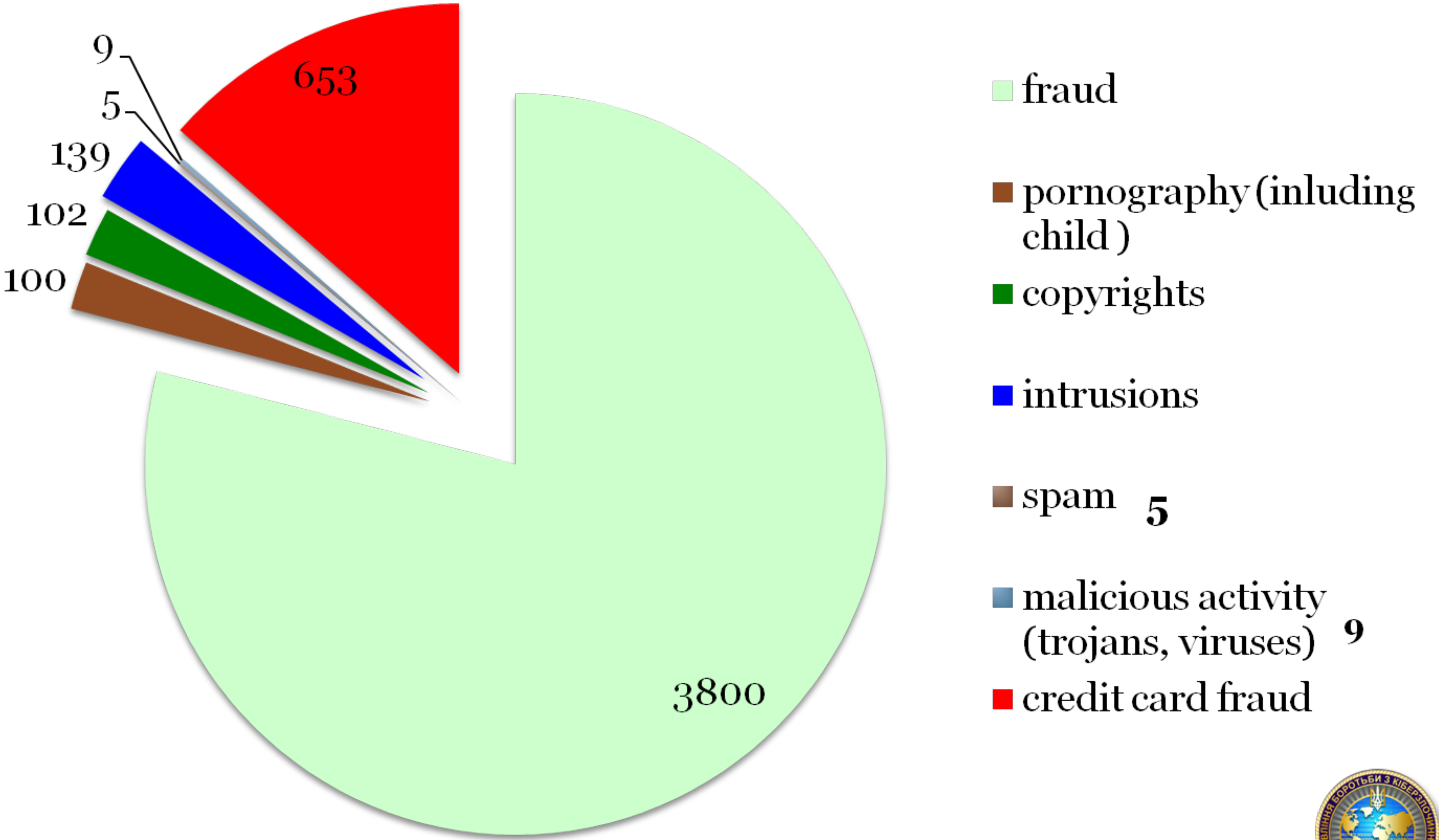
- fraud (including computer-related fraud) – art. 190 CCU;
- using fake payment cards and other payment documents – art. 200 CCU;
- illegal collecting of bank information – art. 231 CCU;
- child sexual exploitation (prostitution, pornography etc.) – art. 301-303 CCU;
- infringement of copyright – art. 176 CCU;
- forgery – art. 358 CCU;
- illegal access and interception – art. 361 CCU;
- spam – art. 363-1 CCU;
- illegal economy activity, gambling– art. 203-1, 203-2 CCU;
- money laundering – art. 209 CCU.

* Security Service of Ukraine (SBU) is able to investigate major cybercrimes if they affect state security

Statistics 2014



Statistics 2015



Our national partners and sources

- State agencies;
- Hosting companies;
- Internet-Service-Providers;
- Commercial banks & bank associations;
- Payment systems;
- Mobile operators;
- Commercial structures;
- NGO's;
- Internet-community.

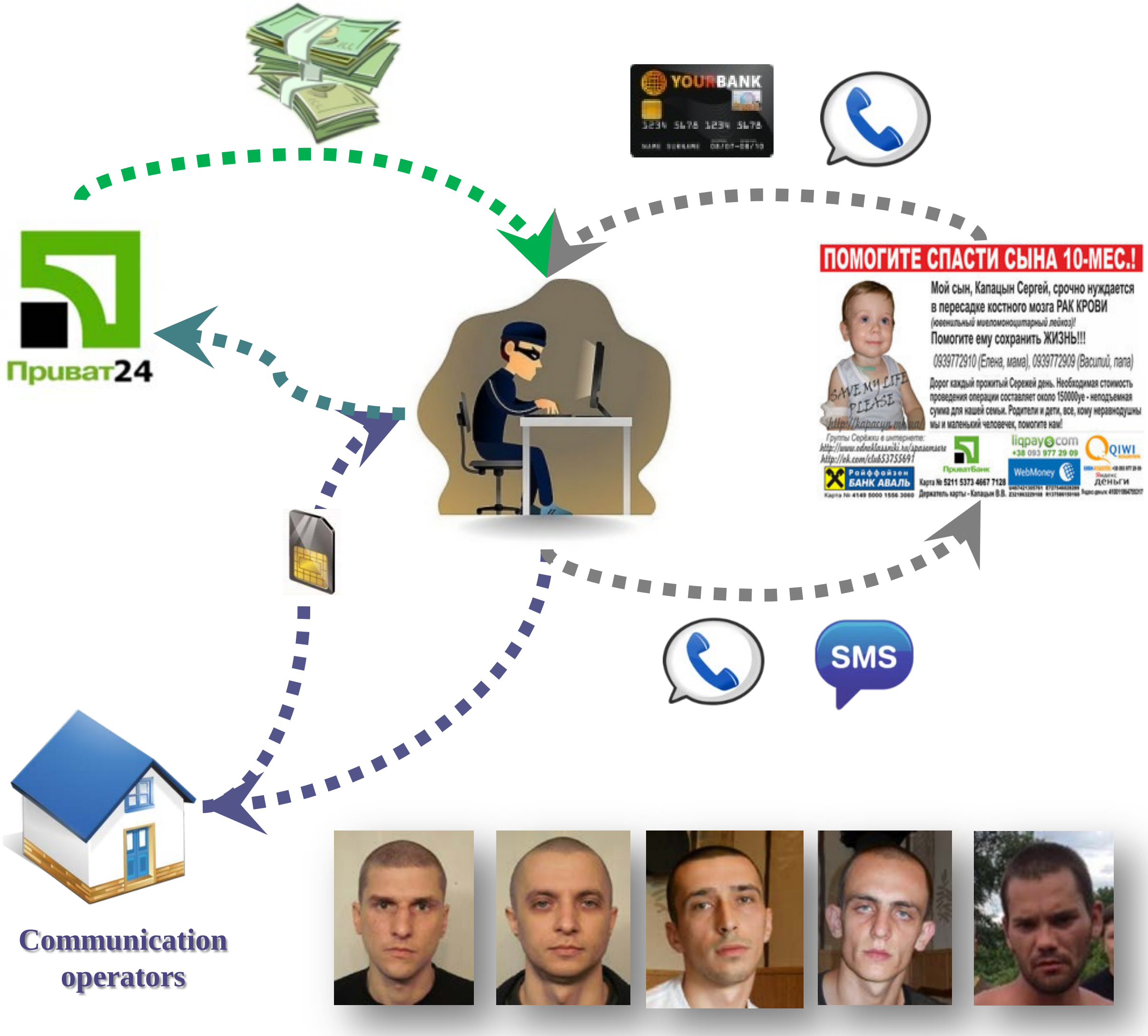
International cooperation

DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION
UNITED STATES SECRET SERVICE
UNITED STATES OF AMERICA EMBASSY
EUROPEAN CYBERCRIME CENTRE EC3 EUROPOL
osce
NCA National Crime Agency
British Embassy
OIPC ICPO INTERPOL
D.C.P.J. OCLCTIC
POLITIE
Bundeskriminalamt

*since 2009 Department on combating cybercrimes established more then 130 strategic contacts with international partners

What we do?

Fraud Case



ПОМОГИТЕ СПАСТИ СЫНА 10-МЕС.!

Мой сын, Капацын Сергей, срочно нуждается в пересадке костного мозга РАК КРОВИ (ювенильный миеломоноцитарный лейкоз)!

Помогите ему сохранить ЖИЗНЬ!!!

0939772910 (Елена, мама), 0939772909 (Василий, папа)

Дорог каждый прожитый Сережей день. Необходимая стоимость проведения операции составляет около 150000уе - неподъемная сумма для нашей семьи. Родители и дети, все, кому неравнодушны мы и маленький человечек, помогите нам!

SAVE MY LIFE PLEASE

Группы Серёжки в интернете:
http://www.odnoklassniki.ru/spasemsere
http://ok.com/club53755691

Райффайзен БАНК АВАЛЬ
Карта № 4149 5000 1556 3060

ПриватБанк
Карта № 5211 5373 4667 7128
Держатель карты - Капацын В.В.

liqpay.com
+38 093 977 29 09

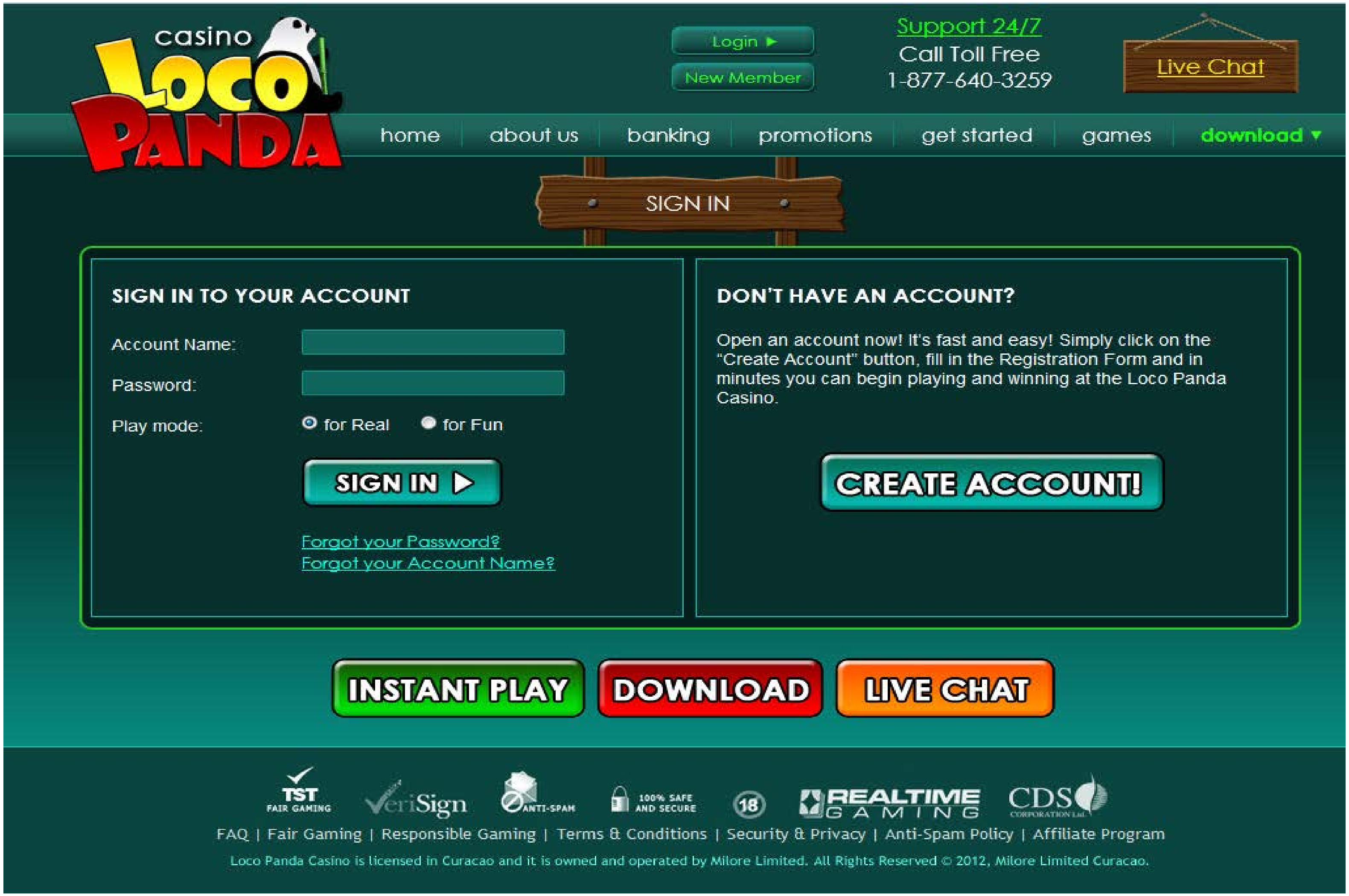
WebMoney

QIWI

Яндекс деньги

1. Suspects collected from the Internet information about volunteers, who was gathering money for children with a cancer;
2. Made a small donation in order to get more info about bank account (cell phone, credit card info etc).
3. Blocked victim’s cell phone and made a sim-cart clone.
4. Stole money from victim’s accounts.
5. More then 80 000$ losses.
6. Victims – 38.
7. All 9 criminals were arrested.

Online gambling



Support 24/7
Call Toll Free
1-877-640-3259

SIGN IN TO YOUR ACCOUNT

Account Name:

Password:

Play mode: ● for Real ○ for Fun

Forgot your Password?
Forgot your Account Name?

DON'T HAVE AN ACCOUNT?

Open an account now! It's fast and easy! Simply click on the "Create Account" button, fill in the Registration Form and in minutes you can begin playing and winning at the Loco Panda Casino.

FAQ | Fair Gaming | Responsible Gaming | Terms & Conditions | Security & Privacy | Anti-Spam Policy | Affiliate Program

Loco Panda Casino is licensed in Curacao and it is owned and operated by Milore Limited. All Rights Reserved © 2012, Milore Limited Curacao.

Child pornography, sexual tourism, grooming

“Deniska” case (pedophile in Vinnitsa)

Cybercrime Division got information from SO-12 BKA of Federative Republic of Germany about messages from Ukraine with proposition of sale child pornography via Internet. To identify a criminal and get evidence Cybercrime Department made an undercover purchase of illegal content.

The seller of pornography was a pedophile and during 2 years committed sexual abuse against pupils of boarding school in Vinnitsa (children from defective families).

3 victims of sexual abuse were identified – boys in the age 8-13 y.o.

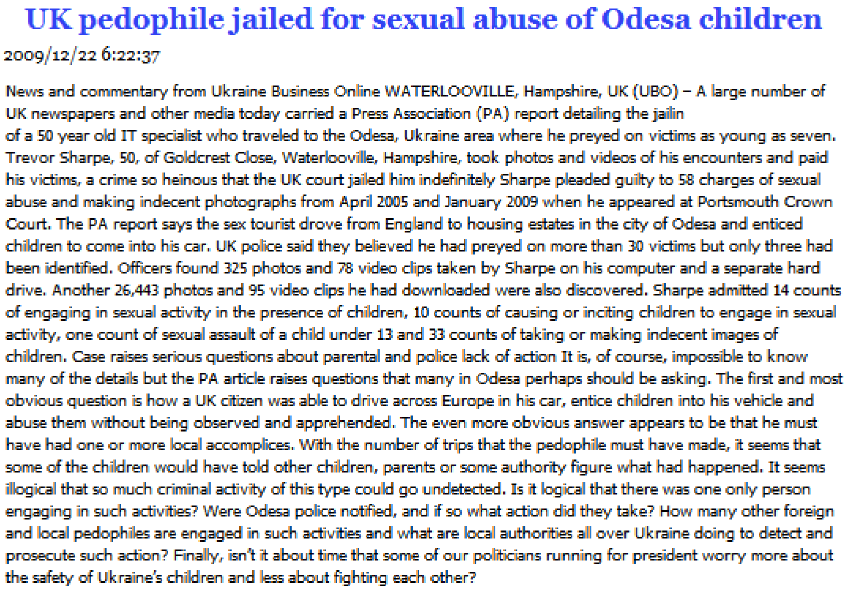
The suspect was arrested. According to court warrant he still in prison.

Traveller pedophile from UK

In close cooperation with UK LEA, Department on combating cybercrimes were able to identified 11 minor victims 0f sexual abuse.

The identification was made by examination background of pictures and video files. Collected information were used in Google Earth software in order to identify the exact place of crimes

As a result of investigation the suspect was jailed in UK.



UK pedophile jailed for sexual abuse of Odesa children

2009/12/22 6:22:37

News and commentary from Ukraine Business Online WATERLOOVILLE, Hampshire, UK (UBO) – A large number of UK newspapers and other media today carried a Press Association (PA) report detailing the jailin of a 50 year old IT specialist who traveled to the Odesa, Ukraine area where he preyed on victims as young as seven. Trevor Sharpe, 50, of Goldcrest Close, Waterlooville, Hampshire, took photos and videos of his encounters and paid his victims, a crime so heinous that the UK court jailed him indefinitely Sharpe pleaded guilty to 58 charges of sexual abuse and making indecent photographs from April 2005 and January 2009 when he appeared at Portsmouth Crown Court. The PA report says the sex tourist drove from England to housing estates in the city of Odesa and enticed children to come into his car. UK police said they believed he had preyed on more than 30 victims but only three had been identified. Officers found 325 photos and 78 video clips taken by Sharpe on his computer and a separate hard drive. Another 26,443 photos and 95 video clips he had downloaded were also discovered. Sharpe admitted 14 counts of engaging in sexual activity in the presence of children, 10 counts of causing or inciting children to engage in sexual activity, one count of sexual assault of a child under 13 and 33 counts of taking or making indecent images of children. Case raises serious questions about parental and police lack of action It is, of course, impossible to know many of the details but the PA article raises questions that many in Odesa perhaps should be asking. The first and most obvious question is how a UK citizen was able to drive across Europe in his car, entice children into his vehicle and abuse them without being observed and apprehended. The even more obvious answer appears to be that he must have had one or more local accomplices. With the number of trips that the pedophile must have made, it seems that some of the children would have told other children, parents or some authority figure what had happened. It seems illogical that so much criminal activity of this type could go undetected. Is it logical that there was one only person engaging in such activities? Were Odesa police notified, and if so what action did they take? How many other foreign and local pedophiles are engaged in such activities and what are local authorities all over Ukraine doing to detect and prosecute such action? Finally, isn't it about time that some of our politicians running for president worry more about the safety of Ukraine's children and less about fighting each other?

AdvancedHosters.com

During the investigation there was sufficient evidence reviled that AdvancedHosters Ltd. supported distribution of prohibited content of child pornography that were located on companies server hardware.

Owners of the company are still at large.

УПРАВЛІННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ © МВС УКРАЇНИ ©

More than 87 Piracy Sources Takedown

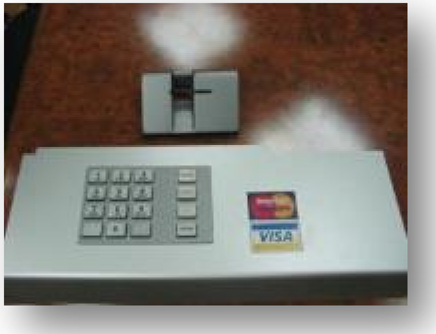
Since 2014 3 big special operations against online piracy industry were held, as a result more then 87 illegal web-sites, file-sharing portals and torrent-trackers were shut down.

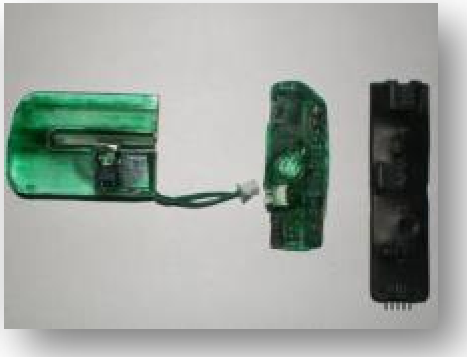
During an action more then 130 servers were seized. After take-down Internet traffic in UA-IX network decreased on 80%.

In Kyiv and Kharkiv organized criminal group was disrupted.

Suspects – two Belarusian and one Ukrainian citizen specialized on payment card fraud. During special operation more then 2500 fraudulent payment cards were seized.

Skimming devises

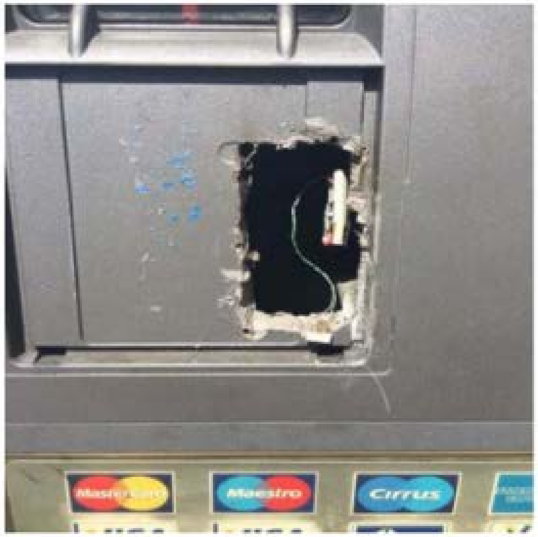




New threat

Eavesdropping attacks

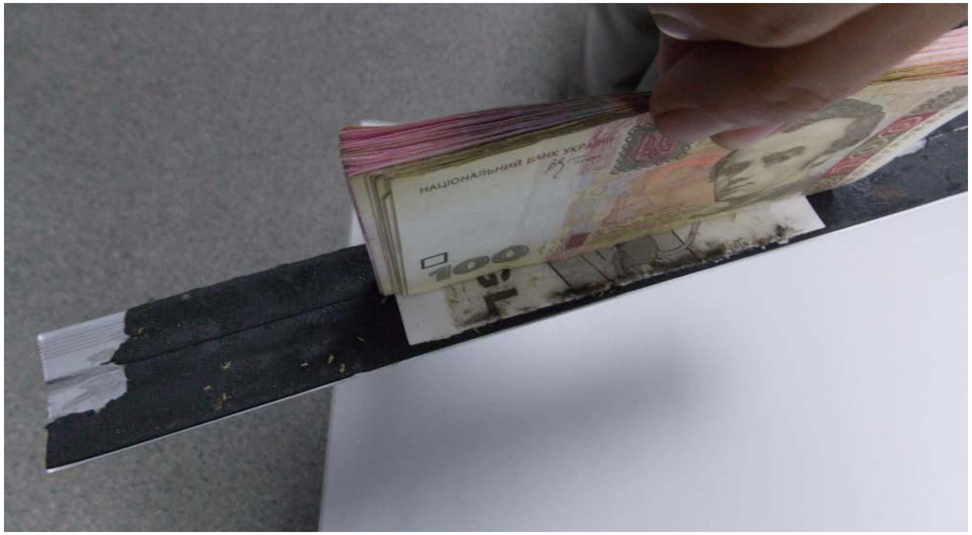
In 2015 new kind of skimmers were discovered. The criminals are gaining access to the card reader by breeching the security of the ATM top box.



ATM Fraud

Cash trapping

Group of suspects detained while they were installing the cash trapping devise in Kharkiv.



Flight tickets fraud

Every year Ukraine take part in special operation hold by Interpol against criminal groups, who specialized on flight tickets fraud

AIR FRANCE

TRANSPORTEUR OFFICIEL - OFFICIAL CARRIER

Міжнародні Авіалінії України

Ukraine International

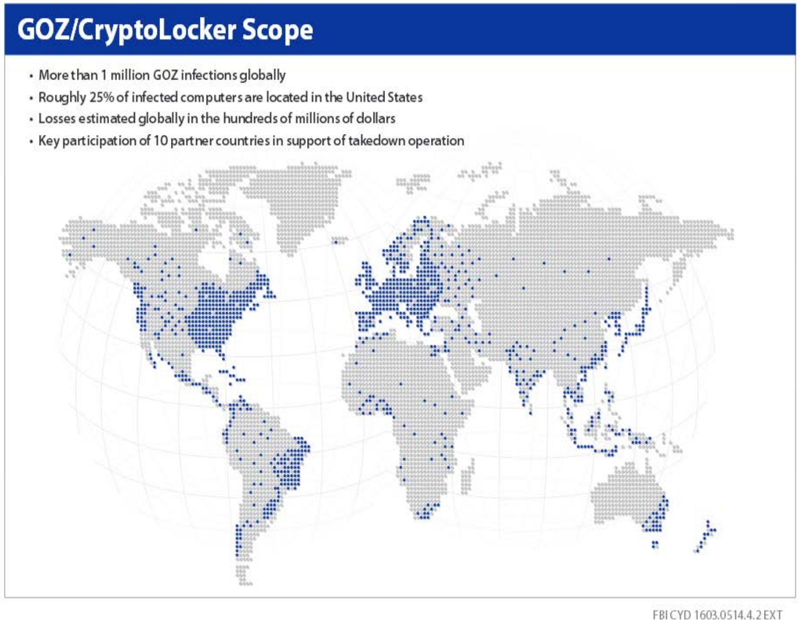
AIRLINES

Lufthansa

АероСвіт

УКРАЇНСЬКІ АВІАЛІНІЇ

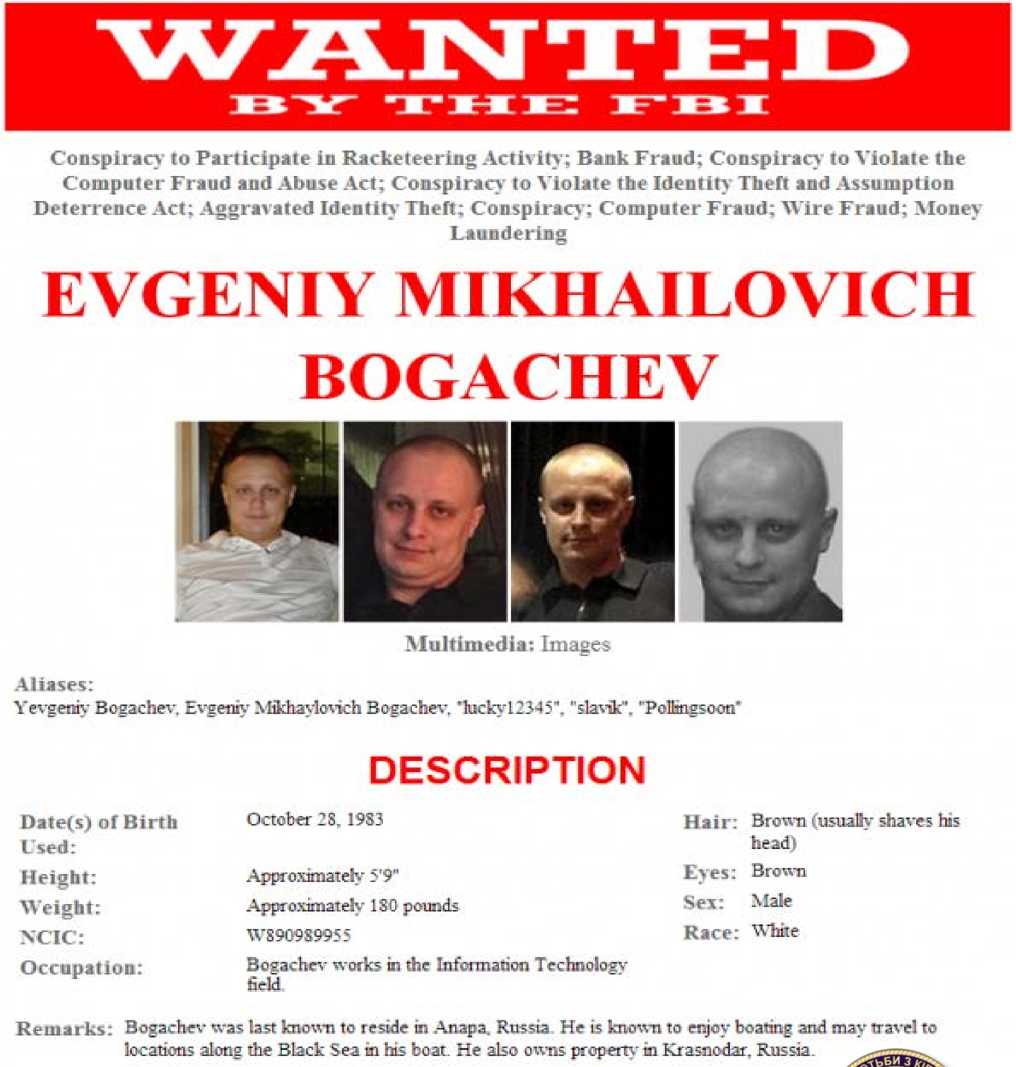
Gameover Zeus and Cryptolocker takedown



GOZ/CryptoLocker Scope

- More than 1 million GOZ infections globally
- Roughly 25% of infected computers are located in the United States
- Losses estimated globally in the hundreds of millions of dollars
- Key participation of 10 partner countries in support of takedown operation

FBI CYD 1603.0514.4.2 EXT



WANTED
BY THE FBI

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering

EVGENIY MIKHAILOVICH BOGACHEV

Multimedia: Images

Aliases:
Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

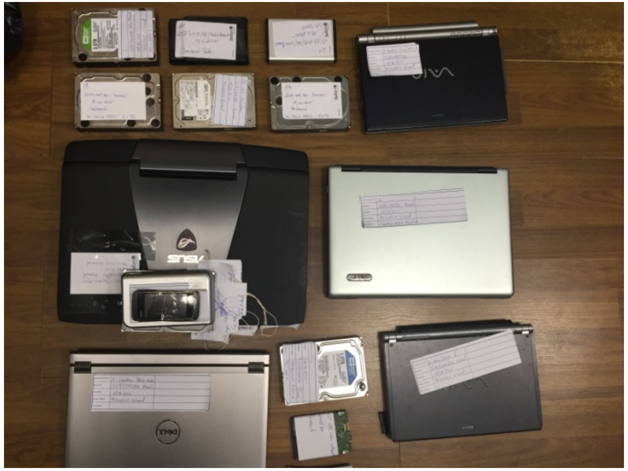
DESCRIPTION

Date(s) of Birth Used:	October 28, 1983	**Hair:**	Brown (usually shaves his head)
Height:	Approximately 5'9"	**Eyes:**	Brown
Weight:	Approximately 180 pounds	**Sex:**	Male
NCIC:	W890989955	**Race:**	White
Occupation:	Bogachev works in the Information Technology field.		

Remarks: Bogachev was last known to reside in Anapa, Russia. He is known to enjoy boating and may travel to locations along the Black Sea in his boat. He also owns property in Krasnodar, Russia.

In 2014 Ministry of Interior of Ukraine in close cooperation with FBI, NCA and Europol, conducted in Ukraine actions against Gameover Zeus botnet and Cryptolocker network

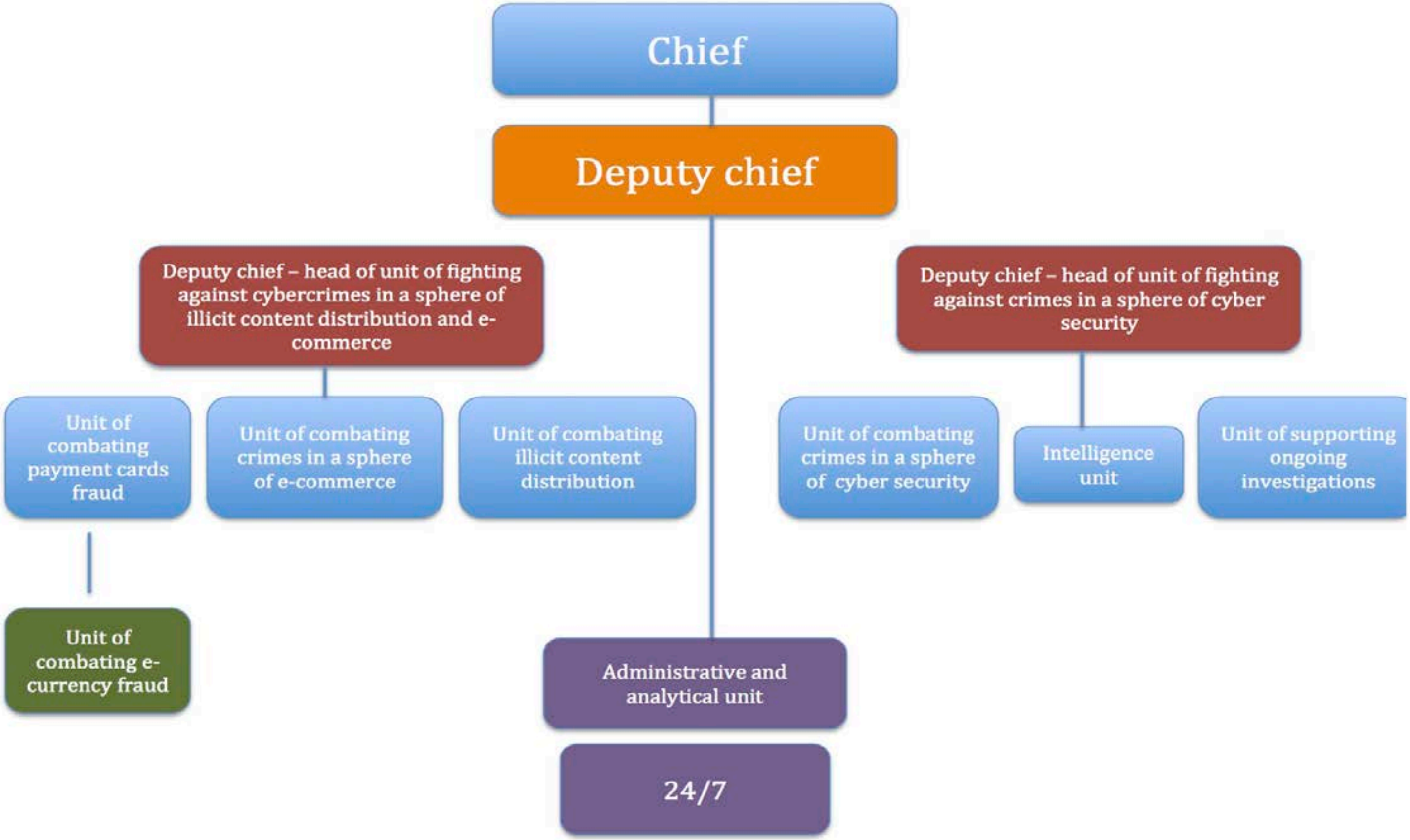
JIT Mozart



A joint investigation team (JIT) consisting of investigators and judicial authorities from six different European countries, supported by Europol and Eurojust, has taken down a major cybercriminal group during a coordinated action in Ukraine. With on-the-spot support from Europol, Austrian and Belgian law enforcement authorities, the action in Ukraine on 18 and 19 June resulted in the arrest of five suspects, eight house searches in four different cities, and the seizure of computer equipment and other devices for further forensic examination.

Strategic plans

Due to ongoing increasing of cybercrimes, new cyber threats, was made decision for restructurisation Department. The new structure will be follow:



Chief

Deputy chief

Deputy chief – head of unit of fighting against cybercrimes in a sphere of illicit content distribution and e-commerce

Unit of combating payment cards fraud

Unit of combating e-currency fraud

Unit of combating crimes in a sphere of e-commerce

Unit of combating illicit content distribution

Deputy chief – head of unit of fighting against crimes in a sphere of cyber security

Unit of combating crimes in a sphere of cyber security

Intelligence unit

Unit of supporting ongoing investigations

Administrative and analytical unit

24/7

QUESTONS?

Vitalii Chubaievskyi
The Chief of the operational and analytical unit
of the Department on combating cybercrimes
MIA of Ukraine