Competent Organizations
In CCTLD

Kalinin Alexander, Head of CERT-GIB
Who is Group-IB?

Group-IB — one of the global leaders in providing high-fidelity Threat Intelligence and anti-fraud solutions

1000+ successful investigations worldwide, 150 of which were of special complexity

$300 million was returned to our clients due to Group-IB's efforts

10000 successful investigations worldwide, 150 of which were of special complexity

$300 million was returned to our clients due to Group-IB's efforts

Media coverage:

- theguardian
- Bloomberg
- Forbes
- Reuters
- Esquire
- CNN
- The Register
- Dark Reading
Group-IB is founded

Group-IB enters the international market

Group-IB computer forensics laboratory becomes the largest in Eastern Europe

Group-IB launches Threat Intelligence

Group-IB launches early warning system for online fraud prevention for banks, payment systems and online resources

Active expansion into international markets

TDS Polygon – a solution designed to detect unknown malicious code by using advanced machine learning algorithms – is introduced into the market

The first product based on the Threat Intelligence system – a detector of threats in corporate networks TDS – enters the market

Computer emergency response team CERT-GIB is established

TDS

 Polygon – a solution designed to detect unknown malicious code by using advanced machine learning algorithms – is introduced into the market

Short history

Group-IB’s extensive experience has developed into an array of highly sophisticated software and hardware solutions based on unique threat intelligence data and incident response in APT threats, allowing the company to identify and prevent cyber threats.

160+ employees

40% software developers

27 average age

45 000 combined hours of response
CERT-GIB (Computer Emergency Response Team) — a round-the-clock computer security incident response team

- Incident monitoring, including distribution of malicious software, phishing, brand abuse, counterfeiting & piracy

- Full legal support on every stage of incident response and investigation

- Professional assistance from specialists with vast experience in response to cyber crime

- Prompt blockage of dangerous websites in the .RU, .РФ domains and other domain zones

- Close cooperation with CERT teams, domain registrars and hosting providers from all over the world

- Collection, analysis and preservation of digital evidences

- Recognized as a competent organization of the Coordination Center for TLD RU (administrator of national top level domains .RU and .РФ)

- Accredited member of FIRST and Trusted Introducer international associations

- Partner of IMPACT — International Multilateral Partnership Against Cyber Threats

- Officially authorized by Carnegie Mellon University and licensed to use the “CERT” trademark in its name
Competent organization from 2011

Group-IB “…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”

We have an Agreement and Regulations in each below listed organization
24/7/365
Russian and English support
More than 10000 suspended domains for 6 years
Who and on what basis?

8 competent organizations:
- Group-IB
- Kaspersky Lab
- The League for Safer Internet
- Regional Public Center of Internet Technology (ROCIT)
- Central Bank of the Russian Federation/Bank of Russia
- Roskomnadzor
- BIZon
- RU-CERT

Specialists for response to technical violations
- Malware analyst
- Forensic specialist
- CERT specialist
- Investigation specialist

Other types of violations
- child pornography
- exhortation for violence and terrorism
- drug distribution
- and other illegal content
Statistics for the half of 2017

From January 1\textsuperscript{st} to September 1\textsuperscript{st} Group-IB suspended in .ru, .su, .рф domain zones:

- More than 1 000 phishing links
- More than 1 000 malware links
- 35 botnet controllers

Also Group-IB helps and supports foreign companies and CERTs in blocking phishing and malware resources hosted or registered in Russia. We proceed more than 2 thousands such requests yearly.

Presence in country of competent for phishing and malware organization allows to shorten the average time of blocking in multiple times.

Types of violations

- Phishing: 50%
- Malware: 48%
- C&C: 2%
What about the Law?

We have some:

- Criminal Code
- Code of Administrative Offenses
- Civil Code
- ...many others

And some problems:

- The vast majority of cases does not fit administrative or criminal law (not 159/272 CC RF) => there is no penalty. As the maximum – penalty according to the civil law.
- The competent authorities doesn’t want to deal with such cases because of their difficulty:
  - Short time of living of phishing sites – it’s hard to collect needed proofs and bring the owner to justice.
  - Hard to identify the owners
  - Problems in definition the victims and their quantity
  - A very long time consideration of such cases and an acute shortage of qualified employees from law enforcement agencies.

The physical threat is minimal, but the virtual one is the maximum in the history of humanity.
Phishing case

Phishing site: «exhibition-2017.ru»
Official site: «exhibition.ru»

Phishing aimed at visitors of the exhibition (large manufacturers)

Collecting data:
• Name, surname;
• E-mail, phone;
• Address of registration;
• Company, position;
• Other personal data.

The fraudster already created 2 similar websites earlier in 2016 year, aimed at another exhibitions.

Suspended for 30 minutes.
Phishing case

Aim: to prosecute the creator.
The creator was identified thanks to Group-IB investigation.

But: law enforcement agencies denied to start a legal case.

Reasons:

• There was no notarial proofs of work of the site. This process takes several days and costs considerable amount of money. During this time the phishing can be removed by the creator (avg. time of phishing life – 2 days);
• It was impossible to proof the fact of collecting personal date because the site was already blocked;
• The damage can’t be estimated;
• It’s really hard to determine visitors who suffered from this site and their quantity.

So… Legal case is even hard to start.
ISP blocking. “Roskomnadzor”

It is also the body administering Russian Internet censorship filters.
Russian Internet Blacklist.

https://eais.rkn.gov.ru/i/slayd.gif
ISP blocking. “Roskomnadzor”

Simplified procedure:
- Using RKN the link with illegal content is blocked for Russian users on the next day after receiving the claim by the court. After this during 30-40 days happens the final blocking of the URL.
- After this the complete blocking of the website is possible, similar procedure.

Objects: films, serials, software, games, books, magazines.

After the enacting the antipiracy law Moscow Court passed more than 400 decisions about blocking. The procedure was applied to the absolute majority of the most popular films and serials that were distributed in Russia.

Advantage: it allow to provide operative protection. Disadvantage: Works only on Russian territory.

Factors that complicates blocking

- Geoblocking
- Filtration by referrer
- Usage of disposable links
- Usage the additional websites from which malware is downloaded
- User-agent filtering
- Usage of iframe
- Temporary availability of the resource
- Usage an additional website for entering confidential data
- Bulletproof registrars and hosters
- Pass-through proxy services that complicates identification of the hoster
- Absense the 24/7 support of hoster/registrar
Yesterday’s case

ICO (Initial coin offering)

- Fraud site (not phishing) distributes through official Telegram channel
- The fraudulent link has been sent repeatedly from accounts that have been renamed to the company's founders' accounts.
- Link was removed from the channel after 7 minutes
- The fraudulent site was blocked for 30 minutes (Russian hosting-provider, Chinese registrar)

$40000 was stolen for 30 minutes
Think about competent organizations

Profit for registrars/registries

1) The competent organization is a your "filter"
2) Reduce the amount of work for the abuse team => lower your costs
3) Increase confidence to your domain zone, as happened with Russia
4) Competent organization - it's free, most often around the clock and multilanguage

Profit for competent organizations

1) The flow of interesting incidents
2) Prestige
3) Social function
4) Improving the quality and speed of work within the country
Please see conference topics and 2016 event review: http://2017.group-ib.com

For any other enquiries, visa and travel support please contact us at cybercrimecon@group-ib.com or call: +7 495 984 3364 (ext. 962)
Questions?

Contact:
Alexander Kalinin
Head of CERT-GIB
kalinin@group-ib.com

www.group-ib.com  info@group-ib.com  twitter.com/groupib
group-ib.com/blog  +7 495 984 33 64  facebook.com/group-ib