RU center

Центр регистрации доменов
www.nic.ru

Internet security in Russia from domain name registrar's and hosting provider's point of view

Alina Legoydo

External representation office of the legal department

Contents:

1. Types of computer incidents registrars and hosting providers deal with
2. Interaction with organizations in Russia fighting illegal activities on the Internet
3. Regulation of Internet activities at the governmental level
4. Cyber security management at the level of registrars and hosting providers
5. Liability of registrars and hosting providers
6. Practical examples of the incidents
7. Conclusion

Computer incidents: Registrars

- Registrars may face a variety of computer security incidents (e.g. domain names with negative associations. For example, childrape.ru, saleofdrugs.ru, etc.)
- Some domains are used for illegal purposes (SPAM, phishing, spreading of viruses)

Widespread illegal activities:

- Illegal seizure of domain names
- Intentional registration of a famous trademark
- Fraud in payment for the domain name or its resale
- Hack of customer personal online account and change of domain settings

Computer incidents: Hosting providers

- face the spread of content, prohibited by law
- face the spread of content violating someone‘s rights
- hosting platforms used as a place to carry out the attacks, theft of funds or information, spread of SPAM
- hosting platforms are attacked to damage the hosting provider (theft of passwords, withdrawal of money from somebody’s account)

E-crime incidents occur:

- against a company by both unauthorized users and dishonourable clients of the company
- against respectable clients by the criminals
- against other Internet users by dishonourable clients

Interaction with organizations fighting against illegal activities on the Internet in Russia

(http://nic.ru/about/no_illegal_content/en/index.html)

- **GROUP-IB and Computer Emergency Response Team (CERT-GIB)**
  http://www.group-ib.ru/

The first and the only non-governmental organization in Russia, which provides consulting services for incidents investigations in the field of information security.
Based on the work of Group-IB the Computer Emergency Response Team was established as a company that promptly reacts to computer security incidents.

- **Hotline of Friendly Runet Foundation**
  http://www.friendlyrunet.ru/

The Hotline's main goal is to purify Runet from illegal content and help users, Internet-industry and governmental authorities to fight the spread of illegal materials of sexual nature with children involved.

Interaction with organizations fighting against illegal activities on the Internet in Russia

(http://nic.ru/about/no_illegal_content/en/index.html)

- **Cybercrime Commission of the Russian Association for Electronic Communications (RAEC)**
  http://raec.ru/

The Association's objective is to create a civilized information society, which will have its own legal system and the codes of professional activities that are to be accepted by both the users and the companies on the Internet.

- **Safety Internet League**
  http://ligainternet.ru/

Reputable association of leading companies and competent public authorities in the Russian Internet and Telecom industry

Regulation of Internet activities at the governmental level

Governmental measures to fight against the spread of illegal information in the Internet:

• Federal Law 149 "On Information, Information Technologies and Information Protection"

• Federal Law 114 “On Counteraction of Extremist Activities”

• Federal Law 139 “On Amendments to Federal Law On Protecting Children from Information Harmful to Their Health and the Development and Certain Legislative Acts of the Russian Federation” (www.zapret-info.gov.ru)

• Draft of the Federal law that would protect the trademark owners (registry of the intellectual property rights). – Drawbacks:
1) No exact process in place to protect TM holders
2) No protection from the uncontrolled interpretation by authorities
3) The impact on the Internet and users has to be investigated

Cyber security management at the level of registrars and hosting providers

Registrars have the direct rights to withdraw the delegation of a domain in case of obvious:

- phishing
- child pornography
- illegal activities

In case of uncertainty, registrar has right to terminate the delegation:

- on demand of organizations fighting cyber crime
- on the court decision (violation of trademark rights)
- request of a law enforcement agency

It is obvious:

- fighting against negative activities alone is inefficient and ultimately inadequate;

- not only observe some initiatives but to participate in their implementation;

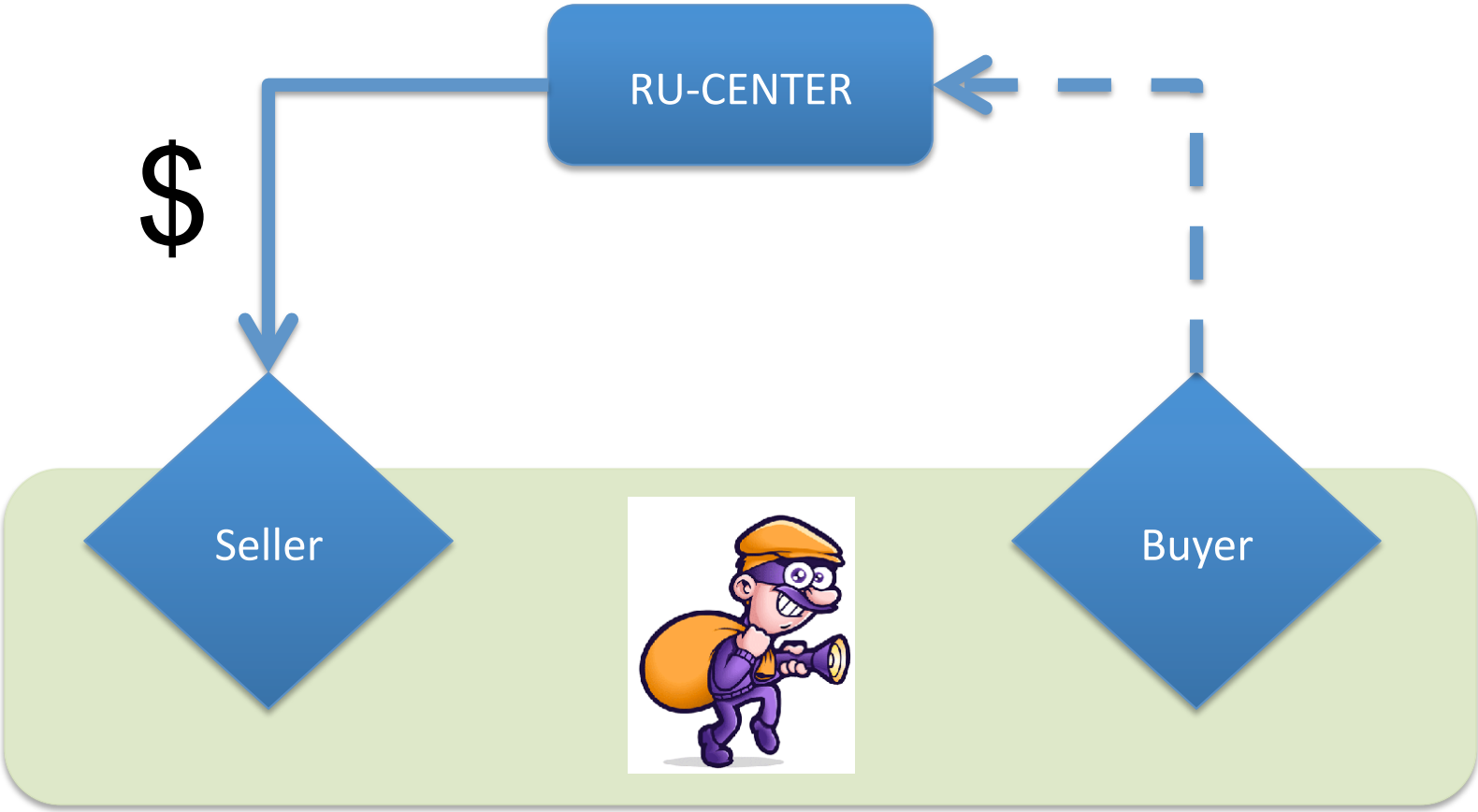
- in taking on the initiatives it is important to take into account the experience and opinions of Internet industry experts;

- keep informed of and learn from international practices as well;

Registrar and hosting provider liability for their clients' actions

"Neither the registrar nor the hosting provider can assume any legal liability, BUT they must have all rights necessary to respond to the actions of their clients, in order to comply with administrative and criminal law, while remaining in a position of strict neutrality."

Case A. Fraud in the resale of domain names



DAMAGE TO THE REGISTRAR

Case A. Fraud in the resale of domain names

A customer has some domains and he puts them up for sale. At the same time he pretends to be a fictional buyer of these domains, usually a non-resident buyer. Using fake data, he makes large payments for the domain names. Upon receiving notice of the transaction, the registrar transferred the money to the seller, who immediately withdrew the money from the account. But through the electronic payment system the money could not be transferred for various reasons, in particular due to fraudulent and criminal activity. Thus, the registrar has already paid the seller so that the domains can immediately be transferred to the buyer and the deal is done but the registrar has never received the money from the buyer. Thus, the unscrupulous owns all of his domains AND got the transferred money from the registrar.

Case A. Fraud in the resale of domain names

Registrar's reaction:

- Lock of customer's account
- Higher security settings in domain name sales and payment operations

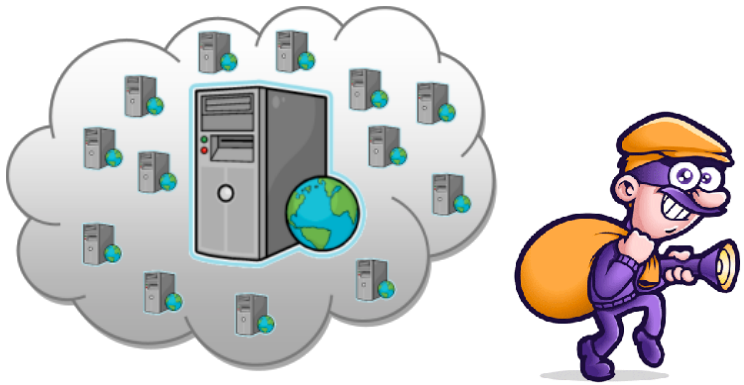
Case B. Unauthorized access to the resources of the hosting provider and registrar

A client with an account on the hosting provider‘s platform conducted a constant scan, looking for the opportunities to change the settings of the various internal corporate provider systems →

Since it was an authorized participant, one of the subsystems perceived his commands →

As a result, he gained an access to the system of domain registration and management of services with extended rights →

The customer illegally ordered additional services, made changes in the contracts, tried to interfere in the operations of the site of a commercial bank



Case B. Unauthorized access to the resources of the hosting provider and registrar

Registrar‘s reaction:

- System administrators have identified these actions and blocked all the accounts of the client

Conclusion

Companies should be aware that:

• Preventing against illegal activities, a company guarantees its own security, the security of its respectable clients and helps law-abiding users;

• Attempting to counter security threats and criminal activity alone is inefficient and inadequate;

• It is important not only to observe some initiatives but also to participate in their implementation;

Conclusion

Companies should be aware that:

•When taking on initiatives it is important to understand and take into account the experience and opinion of Internet industry experts and the guidelines of international practice;

• Neither the registrar nor the hosting provider can assume any legal liability, but they must have all rights necessary to respond to the actions of their clients and to comply with the administrative and criminal law, while remaining in a position of strict neutrality.

• Social responsibility is the foundation for the success in an honest business.

Questions?

Thank you!

e-mail: alegoydo@hostcomm.ru
web: http://ник.рф, http://nic.ru