Cyber attacks in Ukraine during revolution and Russian intervention

Glib Pakharenko
gpaharenko (at) gmail.com

2014-10-13

This is solely my personal opinion
Do not consider as call for any action

Cyber attacks were before the revolution

< 30 November 2013

Cyber attacks was quite popular before the revolution.

- 100Gbit/s Ddos in UA segment in 2010
- politically motivated attacks before elections
  - Ddos on party sites
  - Compromise of accounts of politician
- economically motivated attacks:
  - Ddos, on e-shops before Christmas
  - Mobile operators fraud
  - Carding
  - Internet banking unauthorized transfers
  - Lockers
  - SEO optimization, SPAM, etc.

Police fights with pirated content, unauthorized porno-studios, and online gambling. Used to takes all servers and PC's with them from victim or suspected.

Ddos attacks was most popular during street protest

December 2013-January 2014

The rate of attacks grows enormously (but dropped for Christmas holidays):

- Ddos attacks against opposition media (BlackEnergy, DirtJumper – Russian made);
- Police takes servers from opposition office;
- Personal accounts of opposition politicians hacked;
- Banks, which served accounts of opposition under hacking attacks (unauthorized transfer and then a Ddos to hide the fraud);
- Anonymous attack government sites;
- A "red" alarm level was on UA nuclear stations when protesters took the ministry of energy building, where control systems were located;
- A PC which controls electricity in the city hall was broken, which led to its black-out;
- Malicious traffic from Russia rerouted out of Ukraine through Belarus and Cyprus (HostExploit statistics). ***That's why the first time in recent years, Ukraine was not in the list of countries with boosted cybercrime.***

Mobile technologies were used during the peak of Revolution

ПОГИБШИЕ ВО ВРЕМЯ АКЦИЙ ПРОТЕСТА В УКРАИНЕ
ПОГИБШИЕ ПРЕДСТАВИТЕЛИ СИЛОВЫХ СТРУКТУР

Feb 2014

During the peak of the Revolution mobile technologies was most important:

- Opposition Parliament member phones were flooded with SMS&Calls;
- IMSI catcher mass messaging was used against protesters;
- In West regions (where the Revolution started) in police departments only mobile phones were working (no PSTN or other connectivity);
- Main opposition TV channel was turned off;
- Police planned to turn off mobile connectivity;
- In East regions police used mobile phone to compromise two-factor authentication and gain access to protester account.

Russia occupies Crimea

Feb-March 2014

- Government under attack:
  - Ddos on the parliament site to prohibit law publishing;
  - Ddos on other sites (national security council, president, etc.);
- Physical attack on cabling infrastructure in Crimea;
- Anonymous attack sites of Russian government in Crimea;
- Russia turned-off UA channels in Crimea;
- Broadcasters were unable to take their telecom equipment hosted in Crimea government datacenters;
- Enormous amount of government and personal data from IT systems now in Russian hands;
- Increased amount of GSM fraud from Crimea against UA operators (as UA law enforcement no longer effective there);
- Russian IT-security NGO RISSPA censored anti-war discussions in its forum;
- Mass changes in Wikipedia articles;
- UA broadcasting satellite "Lybid" was not launched, as the space control center was conquered.

War with Russia

April 2014 – till now

Russia effectively use cyber-technology to support their war. Physical attacks are especially dangerous against:

- cabling and broadcast infrastructure in area of fighting (media and financial services unavailable);
- cabling infrastructure in Kyiv (terracts);
- ATMs of specific banks all over Ukraine (terracts).

Mobile technology attacks:

- Used for correction of artillery fire;
- Talks interception;
- Traffic rerouting into Russia using VLR/HRL updates;
- Forensics of devices owned by UA supporters;

Hacking attempts against IT systems of:

- UA officials and businessmen accounts;
- Local and central public administration;
- Electronic election systems (coordinated with Russian main TV channel);
- Railway IT systems;
- Mobile operators;

Russian military activity coordinated with Russian TV channels.

ХАРЬКОВСКАЯ ОБЛАСТЬ
РОССИЯ
ЗАПОРОЖСКАЯ ОБЛАСТЬ

Russia acts

April 2014 – till now

Russia has big potential for future cyber conflict:

- Mass attacks similar (like against Estonia and Georgia);
- Data interception in Russian IT services:
  - Ukrainians use Mail.ru, VK.com, etc.;
  - UA sites have counters (JavaScript)from Yandex;
  - Kaspersky, Dr. Web, 1C, Abby are very popular;
- Russian owns or influence UA:
  - mobile operators (MTS, Kyivstar);
  - IT integrators and distributors (RRC, Jet);
  - Parameters of national encryption standard;
  - Support centers based in Russia (e.g. Arbor);
  - Webmoney (installs their root CA in browser!);
  - SCADA systems produced in Russia;
  - Internet-banking produced in Russia;
  - Anti-Ddos solutions (traffic rerouted to Moscow);
- On the occupied territory:
  - Internet censorship (blocking UA sites);
  - Taking ownership on telecom and media property;
  - UA TV channels are turned off.

Russia acts (continued)

April 2014 – till now

Russian cyber criminals became very active:

- Specialized botnets being created from UA users only;
- Mass attacks against smartphone users over SMS;
- Even Smart TV's were infected and forced to show terrorist channels;

Russian propaganda is very effective:

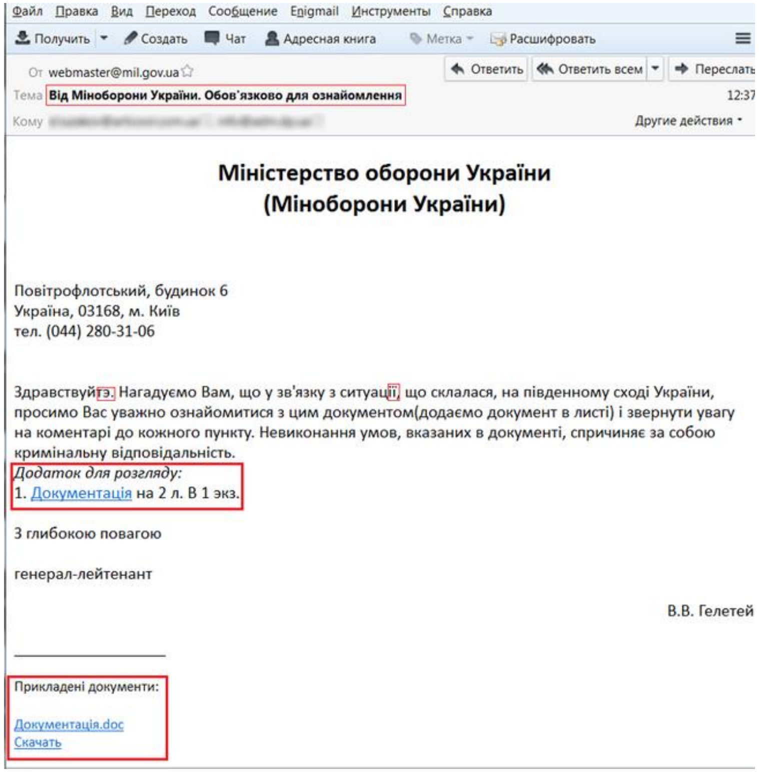
- Thousands of bots and operators work to influence rating and comments in social media or on popular news sites;
- Pro-Russian articles all over the Internet (even on IT sites);

Terrorists use Internet to:

- Recruited new members;
- Communicate with each other in a secure way.

Terrorists warn about bombs in main TV channels in Kyiv.

Examples of attacks linked to Russia



От webmaster@mil.gov.ua

Тема **Від Міноборони України. Обов'язково для ознайомлення** 12:37

Кому [redacted]

Міністерство оборони України
(Міноборони України)

Повітрофлотський, будинок 6
Україна, 03168, м. Київ
тел. (044) 280-31-06

Здравствуйтэ. Нагадуємо Вам, що у зв'язку з ситуації, що склалася, на південному сході України, просимо Вас уважно ознайомитися з цим документом(додаємо документ в листі) і звернути увагу на коментарі до кожного пункту. Невиконання умов, вказаних в документі, спричиняє за собою кримінальну відповідальність.
Додаток для розгляду:
1. Документація на 2 л. В 1 экз.

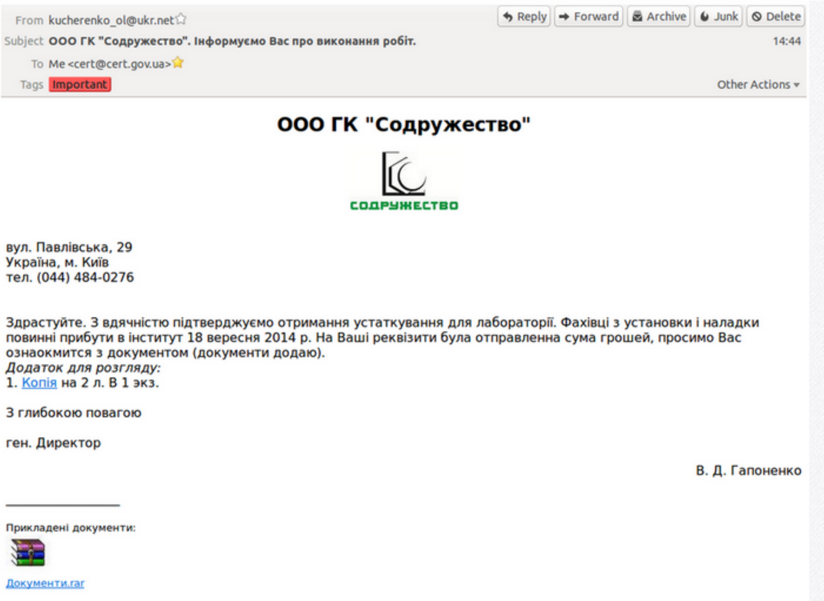
З глибокою повагою

генерал-лейтенант

В.В. Гелетей

Прикладені документи:

Документація.doc
Скачать



From kucherenko_ol@ukr.net

Subject **ООО ГК "Содружество". Інформуємо Вас про виконання робіт.** 14:44

To Me <cert@cert.gov.ua>

Tags Important

ООО ГК "Содружество"

СОДРУЖЕСТВО

вул. Павлівська, 29
Україна, м. Київ
тел. (044) 484-0276

Здрастуйте. З вдячністю підтверджуємо отримання устаткування для лабораторії. Фахівці з установки і наладки повинні прибути в інститут 18 вересня 2014 р. На Ваші реквізити була отправленна сума грошей, просимо Вас ознаокмится з документом (документи додаю).
Додаток для розгляду:
1. Копія на 2 л. В 1 экз.

З глибокою повагою

ген. Директор

В. Д. Гапоненко

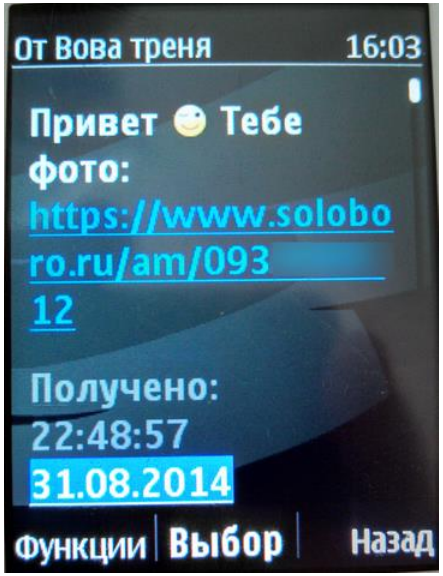
Прикладені документи:

Документи.rar

There are elements indicating the involvement of the Russian in letters

Examples of attacks linked to Russia

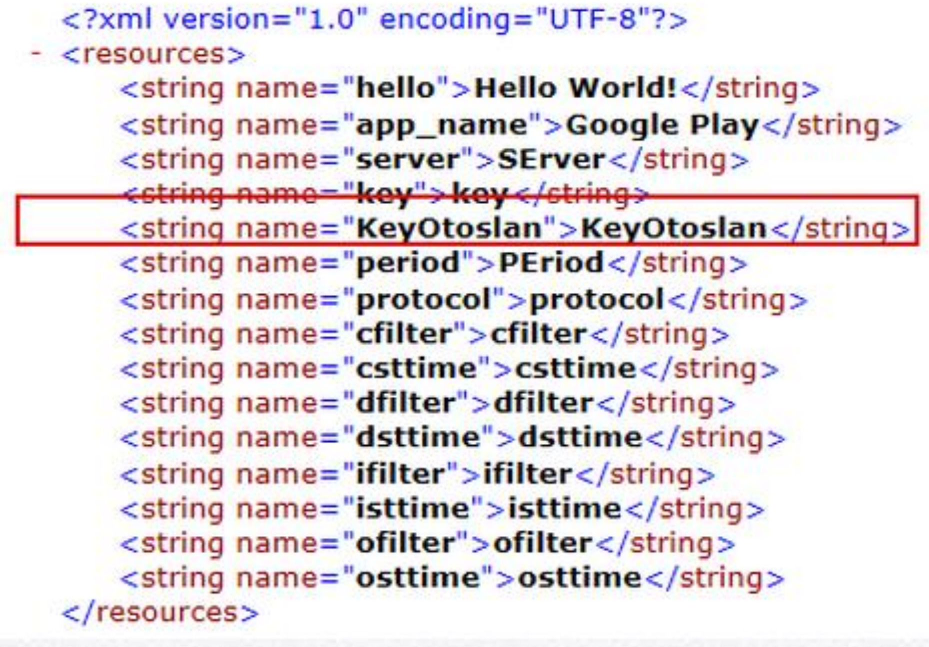
Mass mailing Trojans Android users



От Вова треня 16:03

Привет 😊 Тебе фото: https://www.solobo ro.ru/am/093[redacted] 12

Получено: 22:48:57 31.08.2014



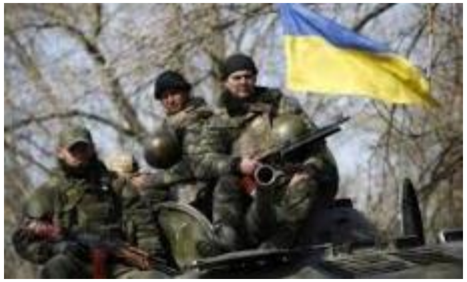
```
  <?xml version="1.0" encoding="UTF-8"?>
- <resources>
      <string name="hello">Hello World!</string>
      <string name="app_name">Google Play</string>
      <string name="server">SErver</string>
      <string name="key">key</string>
      <string name="KeyOtoslan">KeyOtoslan</string>
      <string name="period">PEriod</string>
      <string name="protocol">protocol</string>
      <string name="cfilter">cfilter</string>
      <string name="csttime">csttime</string>
      <string name="dfilter">dfilter</string>
      <string name="dsttime">dsttime</string>
      <string name="ifilter">ifilter</string>
      <string name="isttime">isttime</string>
      <string name="ofilter">ofilter</string>
      <string name="osttime">osttime</string>
  </resources>
```

Some files are signs of Russian-origin

Examples of attacks linked to Russia

Social network Vkontakte used by fraudsters for target viral infection

Ukraine response



April 2014 – till now

Ukraine improves its response in cyber-space:

- Close access to national registers from occupied territories;
- Terrorist communications being intercepted;
- Blocking of terrorist sites;
- Prosecution authors of terrorist content;
- Improve capabilities of CERT-UA team;
- Development of national cyber-security legislation;
- Limiting usage of Russian software;
- Limited usage of mobile phones on war territory;
- Fight with Russian cyber-criminals;
- Increased collaboration between government and private sectors.
- Mobilizaiton of Ukrainian chapters and NGOs like ISACA Kyiv chapter, OWASP, UISG etc. ;
- Volunteers give IT equipment to army.

Even more effort required (lessons learned)

Cyber-war is effectively supports military operations.

- Put cyber-security into your "crisis-plan", when your closest ally becomes an enemy;
- Do not have all your Internet traffic routed through a single neighbor country;
- Clean your country networks (DNS&NTP servers, infected PC, no pirated software);
- Design your web sites to be compatible with anti-ddos solutions (but attacks can flood your office WAN links to defeat anti-ddos service);
- Monitor attacks, exchange information about them, research them;
- Implement effective filtering mechanism on national exchange points;
- Implement BCP plans for media to work in zones of war or terrorist attacks and deliver government information to audience in those areas;
- Have a strong cyber-research capabilities in your country;
- Have a strong national IT services (resist to globalization);
- Implement controls for unauthorized use of lawful interception and cyber-operations by public authorities;
- Implement national security standards acceptable both in public and private sector;
- Make a simple and easy mechanisms for private researchers to get attack details;
- Support creation of many CERT teams as possible;
- Provide military and special forces with capabilities of effective large scale cyber-operations and forensics;
- Prepare for occupation: have encryption, hidden communication with your partners, emergency data erase and quick recovery of IT systems in other geographical region.

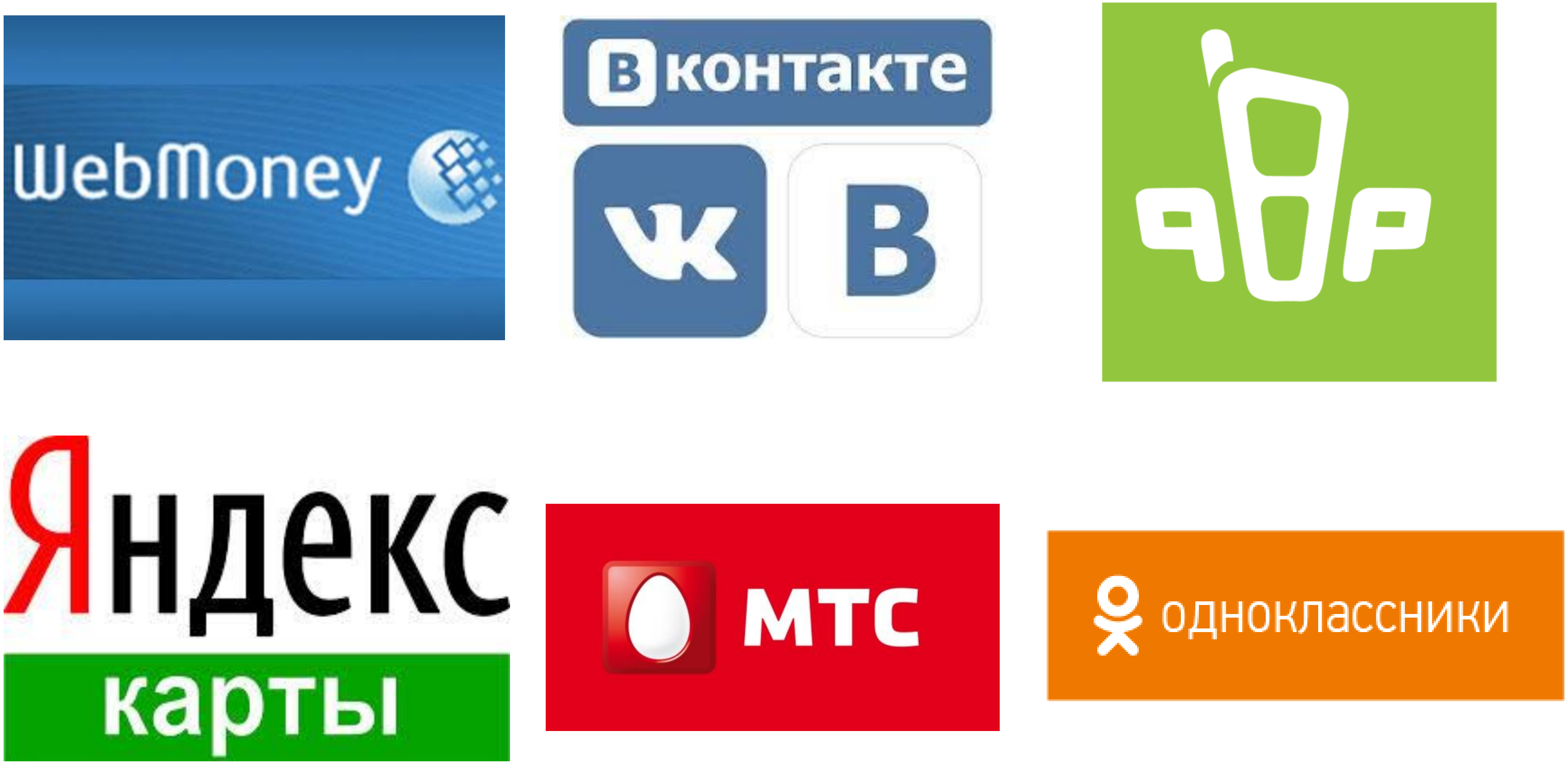
Ukrainians afraid to use “made in Russia”

Might be controlled remotely

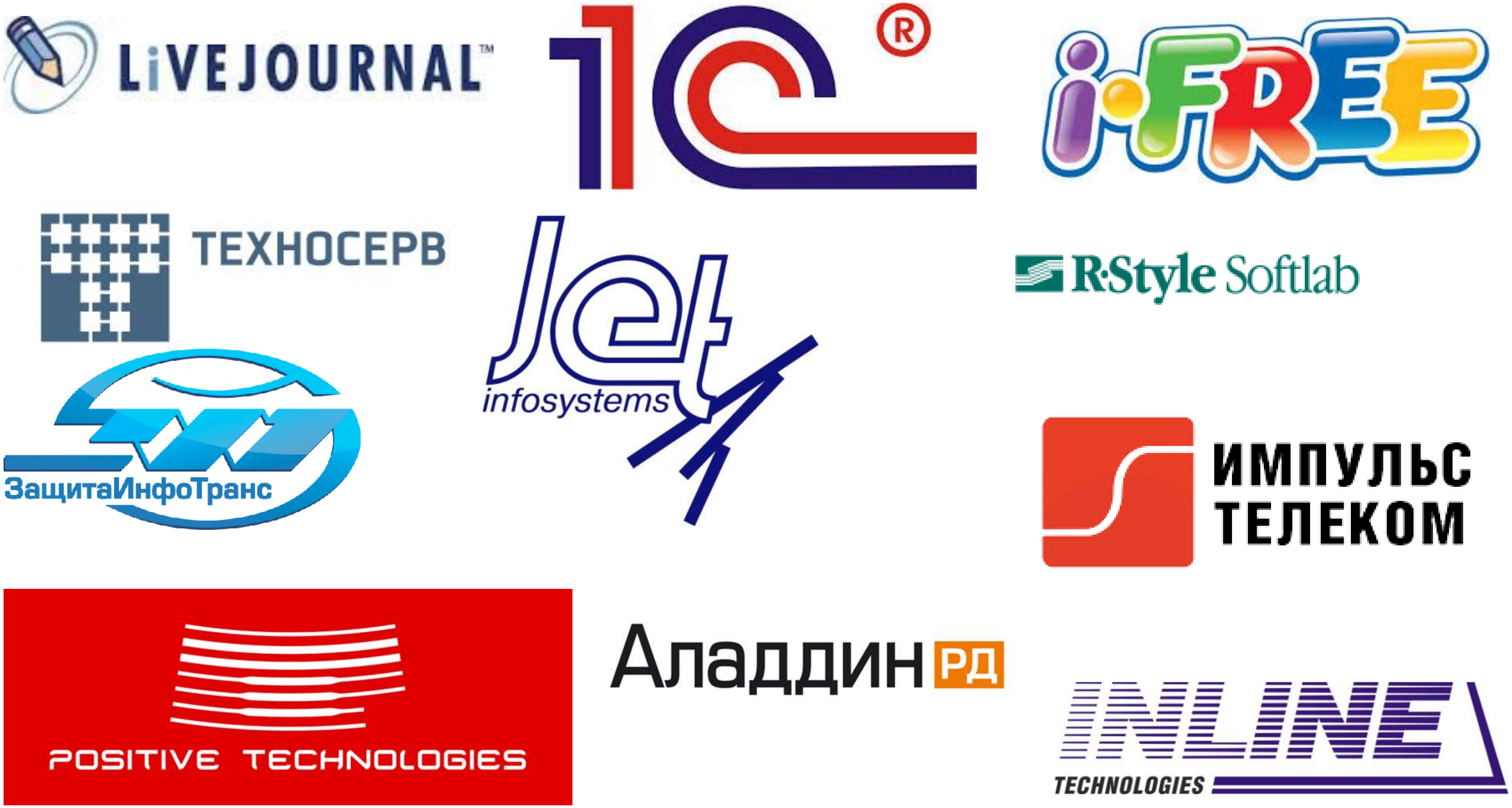
loads javascript code

Ukrainians afraid to use “made in Russia”

Might be controlled by the Federal Security Service



Ukrainians afraid to use “made in Russia”



BE READY TO PROTECT YOUR INDEPENDENCE AND DEMOCRACY

Share your ideas about improving national cyber security capabilities with me
gpaharenko [at] gmail.com