1 October 2009

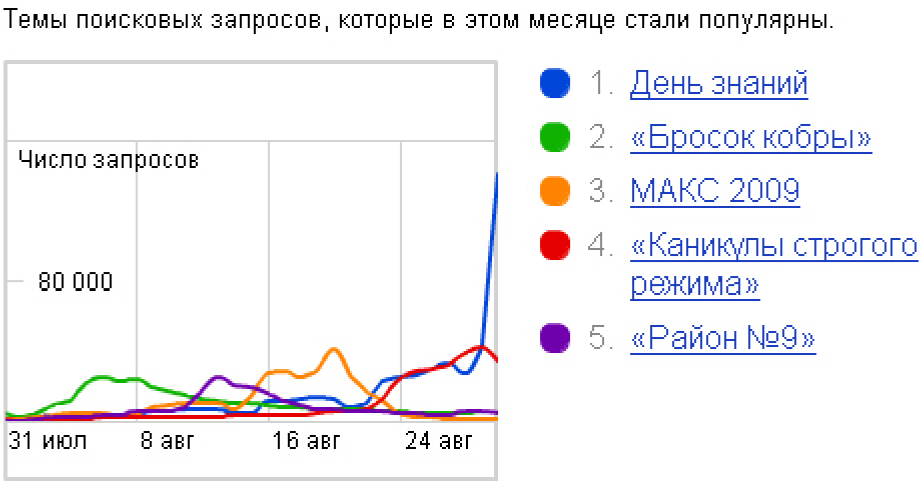
Open Source Center Report

Russia: Cyber Focus, Issue 2

Cyber Focus provides an overview of developments in the Russian-language Internet (or "Runet"). This is the second of three planned pilot editions. We welcome all feedback, which can be sent to CEP-EMT@rccb.osis.gov. This edition includes the following sections:

Snapshot

Yandex Interesy compares search volume patterns across specific regions, categories, time frames and properties. Below are the Russian-language search queries which showed greatest increases over the month of August, an English translation is below the graph.



Темы поисковых запросов, которые в этом месяце стали популярны.

Source: *interes.yandex.ru*, captured 30 September

This OSC product is based exclusively on the content and behavior of selected media and has not been coordinated with other US Government components.

1. Knowledge Day	1 September, first day of school year
2. The Rise of Cobra	2009 US movie
3. MAKS 2009	International air show held near Moscow
4. High Security Vacation	2009 Belarus movie
5. District 9	2009 US movie

Cyber Security and Cyber Crime

Russian State Websites Vulnerable to Attack

Hackers continue to target Russian government websites, including a regional website for the Ministry of Internal Affairs and the Federal Space Agency.

- The official site of the Ministry of Internal Affairs in the North Caucasus republic of Ingushetia (*Mvd-ri.ru*) spent several days offline due to a hacker attack, officials said. BBC Monitoring reported that the site of the President of the Republic (*Ingushetia.ru*) was also offline.[1] The representative of the Ingush President's press service told RIA Novosti that attacks against the MVD site are common (*Gazeta.ru*, 17 September).

- The press service of the Federal Space Agency Rokosmos announced on 9 September that the agency's website had been attacked by a script virus, but did not say when, according to the pro-government website *Vzglyad*. The agency's database was damaged as a result. Andrey Vorobev, the director of the department for public communications stated that the attack was likely the work of a novice hacker testing his skills and opined that the attack posed no threat to the International Space Station (, 9 September).

- On 22 September, anti-government website *Newsru.com* reported that hackers had seized control of the website of the Russian Pension Fund and filled it with senseless text. However, the fund's representative stated that it was simply a technical glitch. On 25 September opposition newspaper *Yezhednevnyy Zhurnal* suggested the filler text had intentionally been used by the Pension Fund website administrators.

[1] See 16 Sep OSC Translation **Two Ingush Official Websites Reportedly Hacked** (CEP20090917950052)

August 2009 DDoS Attack on Ukraine; Further Attacks Expected

Ruformator.ru, a Russian website focusing on developments in the Russian Internet, reported on 23 September that the Ukrainian Internet ("UaNet") had survived the "most powerful DDoS assault in its history" at the end of August.

- The attack targeted domain registry and hosting service *Imena.ua* (and sister site *Mirohost.net.*)
- At the peak of the attack, 26-27 August, the company's server recorded 2GB/s worth of requests.
- The news of the attack was only publicized one month after the fact because the company first notified the Security Service of Ukraine in the hopes of finding those responsible.

The website of the Ukrainian business daily *Delo (Delo.ua)* traced two of the command-and-control IP addresses to the Zeus botnet. *Delo.ua* claimed the attack was a test of strength by hackers preparing for Ukraine's presidential elections in January.

- On 3 August Latvian ISP Real Host was disconnected for directing command-and-control servers for Zeus (*cio.com*, 5 Aug).[2] Despite this, Zeus is believed to currently control 3.6 million computers (*Delo.ua*, 23 Sep). *Ruformator* reported that the botnet "was reconstructed by the end of the month in other countries, particularly China" (23 September).
- *Delo.ua* described the attack as the "first swallow" of the pre-election period. Ukraine's Presidential elections are scheduled for 17 January 2010.
- Sergey Polishchuk, a technical administrator with Ukraine's Internet exchange network UA-IX,[3] said he expects to see DDoS attacks of over 10GB/s "within the next two years" (*Delo.ua*, 23 Sep).

White Hat Hackers[4] Access Source Code of Major Runet Portals

Programmers published vulnerabilities that allowed access to the file structure and, in some cases, the source code of over 3,320 sites including *Yandex*, *Rambler*, *Mail.ru*, *RBK*, Internet stores *003.ru* and *Bolero.ru*, and the Internet browser *Opera.com* (*Infox.ru*, 24 September).

[2] See 7 August OSC Summary **Cyber Threat Media Highlights** (LAP20090810473004)

[3] An internet exchange or IX allows ISPs to reduce costs and bandwidth usage by providing interconnections that are collectively owned and managed.

[4] "White hat" hackers are ethical computer security enthusiasts, distinguished from "black hat" hackers who specialize in unauthorized penetration.

- The programmers reported the vulnerabilities "about two months ago" and released the information into the public domain on 23 September.
- One of the programmers, Anton Isaykin stated that the portals had been informed of the vulnerabilities and that he waited until they had been fixed before publishing the information

LiveJournal Suspends Multimedia after Virus Attack

The popular blogging platform *LiveJournal* was attacked for the first time on 25 September by a virus carried by a video post. The virus, which was written in Flash language, infected the journals of users by changing their settings, opening "locked" posts and stealing their email addresses (*Cnews.ru* , 25 September). *LiveJournal*'s technical team suspended support for audiovisual files but has restored access to *YouTube* and *RuTube* videos (*Ruformator.ru*, 24 September).

Bloggers With Hacking Interest Prefer *Mail.ru, LiveJournal, Blogspot*

Russian hacking enthusiasts have very different blogging preferences compared to the average Russian Internet user. A poll on popular hacker forum *Khaker* (*www.xakep.ru*) asked users "Do you have your own blog?" and received 6,508 responses (*Khaker*, 29 September).

- A large majority of respondents (73%) do not have a blog.
- *Mail.ru* and *LiveJournal* were the two most popular platforms.

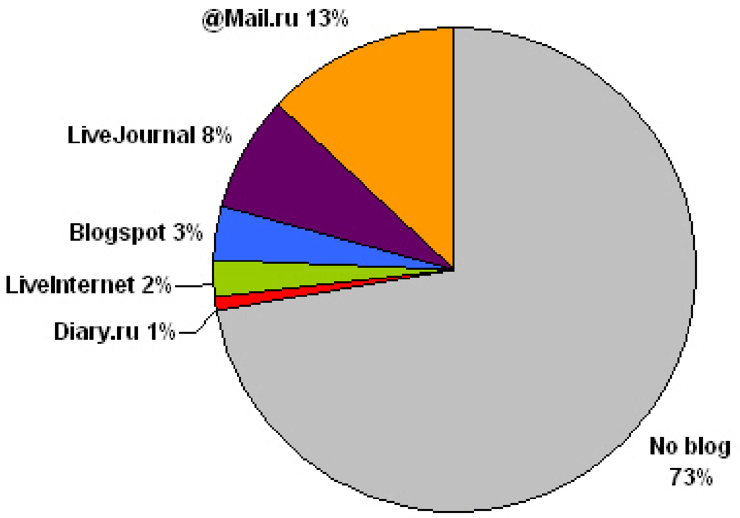
When compared with data from the *Yandex* "Runet Blogosphere Spring 2009" report, preferences of *Khaker* users varied from aggregate figures.

- *LiveInternet*, a major Russian blogging platform with 36% of Russian blogs, was used by only 9% of *Khaker* bloggers.[5]
- *Mail.ru* and *LiveJournal* both recorded a higher proportion of *Khaker* bloggers than average Russian bloggers.
- *Khaker* users are eight times more likely to use *Blogspot*, *Google*'s blogging platform, than the average Russian Internet user.

These variances suggest hacker blogs are most likely to be found on *Mail.ru* and *LiveJournal*. They also suggest hackers may be more informed about non-Russian internet services, as indicated by the relatively high use of *Google* blogging platform *Blogspot*.

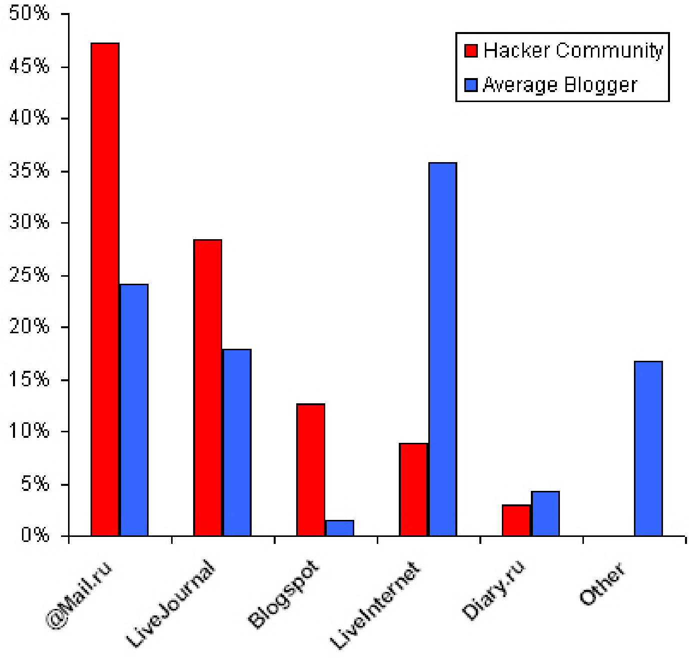
[5] Although *LiveInternet* hosts the largest number of blogs, a relatively high proportion of them lie dormant. *LiveJournal* hosts the largest number of "active" Russian blogs (*Yandex* Runet Blogosphere Spring 2009 report)

Blog Platform Preferences of Hacking Enthusiasts



OSC graphic based on data from *Khaker*

Blog Preferences: Hacking Enthusiasts Compared With Average Russian Blogger



OSC graphic based on data from *Khaker* and *Yandex* Runet Blogosphere Spring 2009 report

This OSC product is based exclusively on the content and behavior of selected media and has not been coordinated with other US Government components.

Russia the Main Source of Fake Anti-Virus Programs.

According to a presentation at the Virus Bulletin 2009 conference in Geneva by anti-virus firm Sophos, Russia is the main source of fake anti-virus programs (*Cnews.ru*, 28 September).

- The report gave details of sophisticated syndication techniques used by Russian spammers, particularly affiliate networks or "partner programs."
- The report stated that most non-email spamming techniques (ie spam on social networks and websites) have not been outlawed explicitly, so spammer groups operate in a legal gray area.
- Spammers use fake anti-virus software to redirect traffic to sites that sell fake anti-virus, pharmaceuticals, and other items to unsuspecting users.

Kaspersky Labs Announces New Patents in Russia

Kaspersky Labs announced on 31 August that it has patented five new information technologies in Russia including a new external anti-virus device and spam filter (*Cnews.ru*, 31 August).

Mobile Telephony

3G Service for Moscow

MTS, Vympelkom, and Megafon plan to offer 3G service in Moscow beginning at the end of 2009 or beginning of 2010. All three conducted tests of compatibility with military technologies and expect to receive permission to use it commercially with some limitations (*Vedomosti*, 3 September).

Censorship & Control

Russia Plans Untraceable Browser for Government Use

The Russian government plans to create a special Internet browser for government employees due to concerns about the security of existing browsers (*Cnews.ru*, 24 September).

- Aleksandr Gridin, the general director of the "Atlas" United Federal Scientific-Technical Center, told the Commission on Federal Communications and Information Technology that it was necessary to develop an anonymous proxy server in Russia that would keep the online activities of government employees from being tracked and analyzed by foreign intelligence services. He elaborated, saying the server would generate the proper amount of masking requests to Internet resources to further complicate any analysis.

- Anatoliy Lakayev, the director of the "Integral" Scientific Research Institute on Special Systems of Communication stated that he was ready to collaborate with "Atlas" and the FSB on the development of the new complex over the next year.
- The platform would be based on Windows or Linux systems incorporating certified cryptographical tools and be based on open-source browser Firefox.

Sergey Mironov Calls for Internet Censorship

The speaker of the Federation Council and leader of the Just Russia party, Sergey Mironov called for censorship on the Internet to protect the populace from "anti-social" sites. He also called for bloggers to agree to a code on tolerant behavior on the net. Mironov singled out criminal sites, pornography sites, websites of drug addicts, sadists, pedophiles, totalitarian sects, as well as the websites of extremist, racist, and nationalist organizations for censorship. The code for bloggers would outlaw "virtual confrontation" but, Mironov stated, would not have any political censorship (*Liberty.ru*, 23 September).

Prosecutor General, Communications Ministry Differ on Internet Filtering

On 17 September the Prosecutor General proposed measures aimed at protecting children from information that is harmful to them and outlawing of the use of the Internet for sexual exploitation of minors and other crimes (*Genproc.gov.ru*, 17 September). However, the Ministry of Communications stated on 23 September that it does not support the proposal, preferring instead to close down illegal sites that contain such content. The ministry agreed with Internet providers, who would be made responsible for content under the Prosecutor General's proposal, that they do not have the necessary technical capabilities or legal rights to control content (*Newsru.com*, 23 September).

Justice Ministry Proposes More Control Over Internet Users

The ministry wants Internet providers to give the law-enforcement agencies information about users and services they are being provided with. Providers may also be ordered to deny access to the Internet to certain users (*Vedomosti*, 29 September)

Bill Proposes USB Modems Registered by Passport

Russian law-enforcers are looking for new ways to control WIFI. The Russian Federal Security Service has drafted a bill which will require registration of passport data to buy a USB modem (*Novyye Izvestiye*, 9 September).

Duma Prepares Law on Electronic Money Transfers

The Committee on Financial Markets is preparing legislation that seeks to regulate financial activity online. The director of the Payment Regulations Department, Alma Obayeva, opined

This OSC product is based exclusively on the content and behavior of selected media and has not been coordinated with other US Government components.

that companies that handle electronic payments should cooperate with banks and that only banks should transfer money (*Newsru.com*, 18 September).

E-Government

With the Russian IT sector dependent on government spending and public procurement processes remaining unreformed, technology companies will almost certainly continue to be susceptible to state influence.

Government Increases Tech Spending

Government spending on technology has continued to grow, and industry support that was earmarked for cuts has not been hit as badly as expected. One of the implications is that many Russian technology companies are highly dependent on continued government support.

- *Cnews* reported that information on the financing of government programs for the development of hi-tech and innovation show a growth of 23% over 2009 (*Cnews.ru*, 25 September).
- Although some cuts were made in the budget and changes were made to the plans, the "Electronic Russia" project will continue and, the Ministry of Mass communications and Telecommunications hopes, lead to the creation of e-Government in Russia (*Cnews.ru*, 17 September).
- Purchases from state bodies make up 25-30% of the IT sector's income, and more than half for 16% of companies surveyed by *Cnews*. Because of the current economic crisis, the number of companies seeking government contracts has gone up dramatically, but the most contracts will continue to go to the current contractors who have experience, a good reputation, and sufficient resources (*Cnews.ru*, 23 September).

Public Procurement Website Still Not Transparent

The latest study by the independent Institute for the Development of Freedom of Information of the ease of access and search for information on official government procurement sites showed that they continue to be largely inaccessible. The overall rating of procurement sites for Russia was just over 50% (*Cnews.ru*, 15 September).[6]

Plan for Online Directory of Government E-Services

A single online directory listing government services accessible through the Internet will be available in the first quarter of next year. Government bodies will decide what information to

[6] See 28 Sep OSC Transcription **Official Websites Of Governmental Procurements Still Far From Perfect** (CEP20090928950189)

This OSC product is based exclusively on the content and behavior of selected media and has not been coordinated with other US Government components.

make available to the population. The goal of the project is to increase the effectiveness of online public services and reduce government expenditure on support of redundant sites (Vesti, 23 September).

Social Networks

Russian Government to Use Blogs as Sources for Ideas

The Ministry of Mass Communications and Telecommunications announced a tender for the creation of a program that would allow federal bodies to search for various useful ideas in social networks (*Molgvardia.ru*, 25 September).

- The authors of the program believe that people talk more freely on the Internet and do not ask for payment for their ideas.
- The proposal calls for the discovery of specialized social networks and the creation of an experimental database of such networks.
- It also calls for the development of a system for monitoring those networks and for the promotion of the interests of federal authorities in them

VKontakte To Expand Overseas, Add New Languages, Allow Filesharing

VKontakte, the popular Russian clone of social networking site *Facebook*, plans to launch 12 versions of itself at the recently acquired domain *http://VK.com*, business daily *Vedomosti* reported on 7 September.

- The new versions are due to come out by October. Although the full list of languages has not yet been announced, OSC observed on 30 September that *VK.com* was offering Englsh, Russian, Ukrainian, Serbian, Polish, and Portuguese.
- It also emerged in early September that *VKontakte* has a new application that allows users to exchange torrent files and download shared files (*Ruformator.ru*, 9 September).

Social Networking Site for Muslims to Be Launched

World-muslim.com, a new Russian social networking site for Muslims, will soon be launched. Although the site is still in testing it is possible to obtain an account for 1 Euro. So far, according to the site, 28,000 people have signed up. The owners and developers of the site have so far opted not to reveal their identities (*Gazeta.ru*, 9 September).

Runet Roundup

The following is a summary of other reports on RuNet developments.

Cyrillic Domains -- Testing in December, Open Registration in Summer 2010

At a session of the Commission on Federal Communications and Information Technology, the director of the Coordination Center of the National Domain of the Internet, Andrey Kolesnikov, announced that the first national language domain would be ready for testing between December 2009 and February 2010 (*Rumetrika.rambler.ru*, 25 September).

- ICANN has said Russia with its .РФ domain (translit. -- .RF) will be the first Cyrillic top-level domain under IPv6. Registration for second-level domains will be open to state bodies Nov 2009 - Mar 2010, then open registration will begin in Apr 2010 (*Vesti*, 24 September).

- Kolesnikov elaborated on the technical aspects of the new domain as well as the limits that will be established in the new domain (*Gazeta.ru*, 15 September). For example, a hacker could be sentenced to up to 7 years in prison for hacking a government information resource (*RBK*, 28 September 2009).

Russia Opposes US Dominance of Internet

The Ministry of Mass Communication and Telecommunications, the Coordination Center of the National Domain, Yandex and RosNIIRos want to break the US monopoly on the management of the Internet. The current agreement on the structure of ICANN is due to expire on 30 September. Russia is in favor of a change in the agreement under which the US holds the majority rights on regulating the Web (*Cnews.ru*, 28 September).

Sberbank Buys Stake in Yandex

Sberbank, a state-owned, public bank, has recently purchased the "gold share" in Yandex, which enables it to veto any sale of more than 25 percent of Yandex shares. As a result, the state has gained assurance that the strategic asset will remain under Russian control. Sberbank received the stake at the symbolic price of 1 Euro (*Vedomosti*, 24 September).[7]

Russia Promises Not To Touch Skype

Despite proposals to limit Skype's activities and use in Russia over security concerns, the Minister of Mass Communications and Telecommunications, Igor Shchegolev stated that there are no plans to block access to Skype (*Vedomosti*, 3 September)

[7] See OSC Translation, **Sberbank To Buy Yandex** (CEP20090924046007)

This OSC product is based exclusively on the content and behavior of selected media and has not been coordinated with other US Government components.