Open Source Center

OSC Report: Russia -- Cyber Focus Issue 1

CEP20090925050001 *Russia -- OSC Report* in English 07 Aug 09 - 22 Aug 09

[For assistance with multimedia elements, contact OSC at 1-800-205-8615 or oscinfo@rccb.osis.gov.]

***Russia:* Cyber Focus, Issue 1**

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

1. Snapshot

2. Cyber Security

3. Social Networks

4. E-Government

5. Runet Roundup

Snapshot -- Online Dialogue at a Glance

Google Insights compares search volume patterns across specific regions, categories, time frames and properties. Below are the Russian-language search queries which showed greatest increases during the week 15-22 August over the previous week, as sourced at http://www.google.com/insights/search/#

Search Terms	Related To
1. Sayano-Shushensk GES	17 August blast at hydroelectric power station
2. District 9 download	American movie
3. Russia-Argentina	Soccer match
4. Maks 2009	16 August midair collision at airshow
5. Godaddy coupon codes	Internet domain registrar

Cyber Security

Respected Russian computer security firm Kaspersky Labs has asserted that malicious botnets are proliferating online and increasingly available for rent. Such botnets may have been behind recent DDoS attacks, such as the campaign against a vocal Georgian blogger that affected *Twitter*, *Livejournal*, *Facebook,* and several *Google* websites.

Kaspersky Labs Publishes Cyber Security Report

On 17 August Kaspersky Labs published a report entitled "Second Quarter 2009: The Web 2.0 Battlefield,"[1] which summarizes recent developments in cyber security. The report said:

- "Daily attacks on social networks have practically become the norm" because of high trust levels between users. Apparently malware spreads through social networks "10 times more effectively" than through e-mail.
- For the first time a worm has surfaced that spreads via microblogging platform *Twitter,* which edits users' personal details on social networks sites. Kaspersky Labs has labelled the worm *Net-Worm.JS.Twettir*.
- The number and size of active botnets continues to grow, and botnet masters are increasingly turning to a scheme known as "Botnet as a Service" (BaaS), which involves renting out botnets for distributed use.
- Kaspersky Labs believes Kido (aka Conficker) to be the largest botnet at present.

The report described the practice of SMS-billing as "specifically Russian," where victims of malware are blackmailed into sending a text message to a premium rate phone number.

- Two SMS-billing trojans with a Russian interface have been reported, classed by Kaspersky Labs as *Trojan-Ransom.Win32.Blocker* and *Trojan-Ransom.Win32.Smser*.
- Both trojans work by blocking an operating system from launching and asking users to send a text message to a premium phone line in order to receive an unblock code.
- Many users do not realize they have been scammed and are tricked into believing they have been penalized for using unlicensed software.

Georgian Blogger at Center of DDoS Attacks Revealed

On 12 August independent website *Gazeta.ru* revealed the identity of Georgian blogger Cyxymu as Giorgi Jakhaia (Russian -- Dzhakhaya), assistant economics professor at Sukhumi State University, Tbilisi.[2]

- Jakhaia describes himself as an Abkhazian refugee and has been an outspoken online critic of Russia's role in the August 2008 conflict.
- Jakhaia's various online profiles were the target of August 2009 DDoS attacks on *Twitter*, *Livejournal*, *Facebook* and several *Google* websites, alongside a spam campaign executed in his name.

Social Networks

BOTh government agencies and hackers are showing an interest in the value of information held by social networks. The Internal Affairs Ministry's public rebuke of Russian *Facebook* clone *Vkontakte* for hosting child pornography suggests increased police interest in the activity of social networks. Meanwhile, hacker groups are using phishing websites to steal social network passwords and charging users to regain access to their profiles.

Police Criticize Social Network for Child Pornography

On 7 August Russia's second largest social network, *VKontakte*, found itself at the center of a child pornography scandal.

- Russia's Ministry of Internal Affairs (MVD) publicly criticized *VKontakte* for failing to control the dissemination of child pornography.
- Apparently over half of the 1,409 pornographic resources closed down at the beginning of 2009 were hosted on *Vkontatke*.
- Rival website *Mail.ru* faced similar allegations in April, when it was accused of tolerating material with "child and infant" pornography.

The accusations came from the MVD's Internet security unit known as Administration K, working with the noncommercial "Druzhestvenniy Runet" (Friendly Runet) foundation.

- The normally secretive Administration K publicized its findings through spokesperson Irina Zubareva, who spoke to *Gazeta.ru* and privately owned news agency *Interfax*.
- Friendly Runet is a project "actively supported" by several federal agencies and "partnered" with 18 telecom and Internet companies (Gazeta.ru, 7 August).

Social Network Login Details Published

Vkontakte found itself in the news again when scammers acquired login passwords to approximately 40,000 active accounts in an apparent phishing operation.[3]

- Attackers used a *Vkontakte* profile to upload interactive games that included hidden malicious code designed to compromise web browsers.
- Users on infected computers who tried to access *Vkontakte* were redirected to a replica "phishing" website hosted in Hausham, Germany.
- Hacking and computer security enthusiast website *Antichat* was apparently the first to locate at least some of the malicious files used.
- *Vebplaneta* blamed *Antichat* members for releasing the stolen account information, stating that "the source of this wave is located on Antichat.ru."
- Reports suggest that users whose accounts were compromised were forced to pay $10 to the attackers in order to regain control of their accounts

E-Government

Despite ambitious promises, Russian Government plans for comprehensive online public services continue to come up against obstacles.

E-Government Plans Fall Behind Schedule

With plans to offer e-government services online by 1 January 2009 already far behind schedule, Communications Minister Igor Shchegolev has suggested transferring current e-government infrastructure to state-controlled Rostelekom (*CNews.ru, 14 August).*

- *President Dmitriy Medvedev and Prime Minister Vladimir Putin have apparently already approved the proposal.*
- *A revised schedule suggests information services should be online by 2010, and remaining services by 2011.*

Declining Interest in Government Websites

Russian Internet portal Rambler reported that in the year ending July 2009, the number of search queries looking for online government services fell by a third year-on-year. Although federal bodies are required by law to keep their websites regularly updated, the report notes that "there are practically no state services that can be obtained [...] without a direct visit [in person] to a state organ" (Rambler.ru, 18 August).

Runet Roundup

The following is a summary of other reports, translations, and OSC products on Russian-language cyber affairs.

Arrest Warrant Issued for Creator of Nationalist Internet Project

A Moscow court approved a Federal Security Service (FSB) request to arrest Anton Mukhachev, a nationalist activist suspected of creating the Internet project known as "The Big Game" which encouraged users to execute real-life acts of violence against ethnic minorities (Forum.msk.ru, 11 August).

Internet Journalist Charged With Libel

Mikhail Afanasyev, editor of the Internet journal Novyy Fokus, has been charged with libel for distributing "intentionally false reports" about the Sayano-Shushensk dam disaster when prosecutors in Khakassia say he was in full possession of "reliable and official information" (Window on Eurasia, 20 August).

Train Tickets Used in Credit Card Fraud

Russia's Internal Affairs Ministry is investigating the use of online rail ticket purchases for credit fraud. Three Volgograd residents were accused of purchasing train tickets online worth over R1.3 million and then collecting the money by canceling the tickets (NEWSru.com, 20 August).

State Bodies Switch to Open Source

There are further signs that Russian state bodies are shying away from commercial software in favor of free, collaboratively produced alternatives. Russia's Federal Agency for Education has asked for tenders for a six-week program to train 60,000 teachers and 7,500 consultants to use free open source software in education. The call for tender came a week after the Federal Bailiffs Service announced it had switched its systems entirely to open source software (CNews, 19 August).

State-Controlled Telco Seeks Increased Subsidies

State-controlled Svyazinvest wants compensation for the burden of providing a telegram service, and has asked the Russian Government to include telegrams as a "universal communication service." This would allow Svyazinvest seek federal subsidies to offset the estimated R2.2 billion loss the company incurs every year providing the service (Kommersant, 20 August).

WiMAX Providers Must Use Russian Hardware

Russia's Ministry of Communications and Mass Media has ruled that telecom operators bidding for bandwidth must commit to providing their services on domestically produced equipment. The bandwidth allocation of 2.3-2.4 GHz covers the provision of WiMAX wireless data transmission in 40 regions (CNews, 20 August).

Children's Browser With Controlled Content Released

Russian company Novoye Pokoleniye[4] released a browser designed specifically for children, allowing access to only 7,000 Russian-language sites. That number is expected to increase as Russian parents, teachers, and child psychologists find suitable pages to add. Some pro-government and patriotic websites are included on the current list (RIA Novosti, 13 August).

[1] *For full report see http://www.securelist.com/ru/analysis/208050541/Vtoroy_kvartal_2009_pole_bitvy_W eb_2_0*

[2] *For more see http://www.gazeta.ru/politics/2009/08/12_kz_3235490.shtml*

[3] *See 14 August OSC Analysis* ***Hacker Group Released Stolen Vkontakte Account Information*** *(CEF20090814592001)*

[4] *The browser's official website can be found at http://gogul.tv*

Submit Review

UNCLASSIFIED