Spy Files Russia

This publication continues WikiLeaks' Spy Files series with releases about surveillance contractors in Russia.

While the surveillance of communication traffic is a global phenomena, the legal and technological framework of its operation is different for each country. Russia's laws - especially the new Yarovaya Law - make literally no distinction between Lawful Interception and mass surveillance by state intelligence authorities (SIAs) without court orders. Russian communication providers are required by Russian law to install the so-called SORM (Система Оперативно-Розыскных Мероприятий) components for surveillance provided by the FSB at their own expense. The SORM infrastructure is developed and deployed in Russia with close cooperation between the FSB, the Interior Ministry of Russia and Russian surveillance contractors.

Releases ▼ **Documents ▼**

All Releases

PETER-SERVICE - 19 September, 2017

PETER-SERVICE

19 September, 2017

English | Русский

Today, September 19th 2017, WikiLeaks starts publishing the series "Spy Files Russia" with documents from the Russian company Петер-

Leaked Documents

for billing solutions and soon became the major supplier of software for the mobile telecommunications industry in Russia. Today it has more than 1000 employees in different locations in Russia, and offices in major cities in Russia and Ukraine. The technologies developed and deployed by PETER-SERVICE today go far beyond the classical billing process and extend into the realms of surveillance and control. Although compliance to the strict surveillance laws is mandatory in Russia, rather than being forced to comply PETER-SERVICE appears to be quite actively pursuing partnership and commercial opportunities with the state intelligence apparatus.

As a matter of fact PETER-SERVICE is uniquely placed as a surveillance partner due to the remarkable visibility their products provide into the data of Russian subscribers of mobile operators, which expose to PETER-SERVICE valuable metadata, including phone and message records, device identifiers (IMEI, MAC addresses), network identifiers (IP addresses), cell tower information and much more. This enriched and aggregated metadata is of course of interest to Russian authorities, whose access became a core component of the system architecture.

Selected components of PETER-SERVICE software

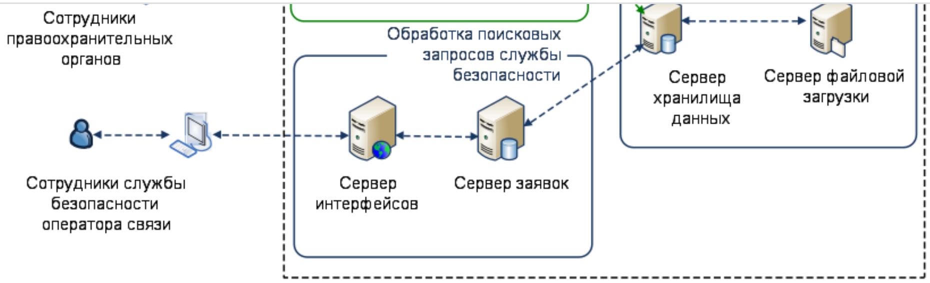
(ЯДРО) СЕМЕЙСТВА ПРОДУКТОВ SPS (G3, v17.0, RUS)

DOC ОСНОВНЫЕ ПОДСИСТЕМЫ (ЯДРО) СЕМЕЙСТВА ПРОДУКТОВ SPS (L6, v5.0, RUS)

DOC ОСНОВНЫЕ ПОДСИСТЕМЫ (ЯДРО) СЕМЕЙСТВА ПРОДУКТОВ SPS (PP, v8.0, RUS)

DOC ОСНОВНЫЕ ПОДСИСТЕМЫ (ЯДРО) СЕМЕЙСТВА ПРОДУКТОВ SPS (GLOSS, v6.0, RUS)

See more


Сотрудники правоохранительных органов
Обработка поисковых запросов службы безопасности
Сервер хранилища данных
Сервер файловой загрузки
Сотрудники службы безопасности оператора связи
Сервер интерфейсов
Сервер заявок

The base architecture of the software from PETER-SERVICE (SVC_BASE) includes components for data retention (DRS [en], [ru]), long-term storage in *SORM* (SSP, Service СП-ПУ), IP traffic analysis (Traffic Data Mart, TDM) and interfaces (adapters) for state agencies to access the archives.

Traffic Data Mart (TDM)

The Traffic Data Mart is a system that records and monitors IP traffic for all mobile devices registered with the operator. It maintains a list of categorized domain names which cover all areas of interest for the state. These categories include blacklisted sites, criminal sites, blogs, webmail, weapons, botnet, narcotics, betting, aggression, racism, terrorism and many more. Based on the collected information the system allows the creation of reports for subscriber devices (identified by IMEI/TAC, brand, model) for a specified time range: Top categories by volume, top sites by volume, top sites by time spent, protocol usage (browsing, mail, telephony, bittorrent) and traffic/time distribution.

Data Retention System (DRS)

The data retention system is a mandatory component for operators by law; it stores all communication (meta-)data locally for three years. State intelligence authorities use the *Protocol 538* adapter built into

Service СП-ПУ

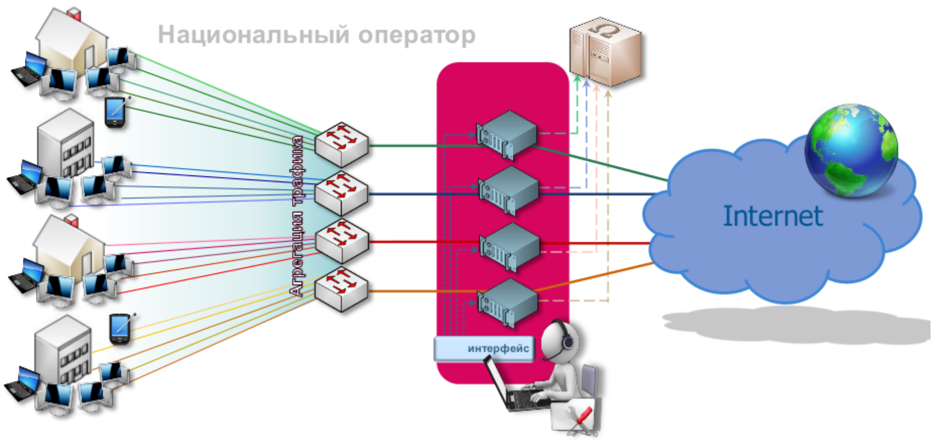
In *SORM* call monitoring functions are concentrated in control points (пунктах управления, ПУ) which are connected to network operators. The Service СП-ПУ is a data exchange interface based on HTTPS between components in SVC_BASE/DRS and *SORM*. The interface receives search requests from state intelligence authorities and delivers results back to the initiator. Search requests for lawful interceptions (based on a court order) are processed by the operator on the same system.

Deep Packet Inspection products

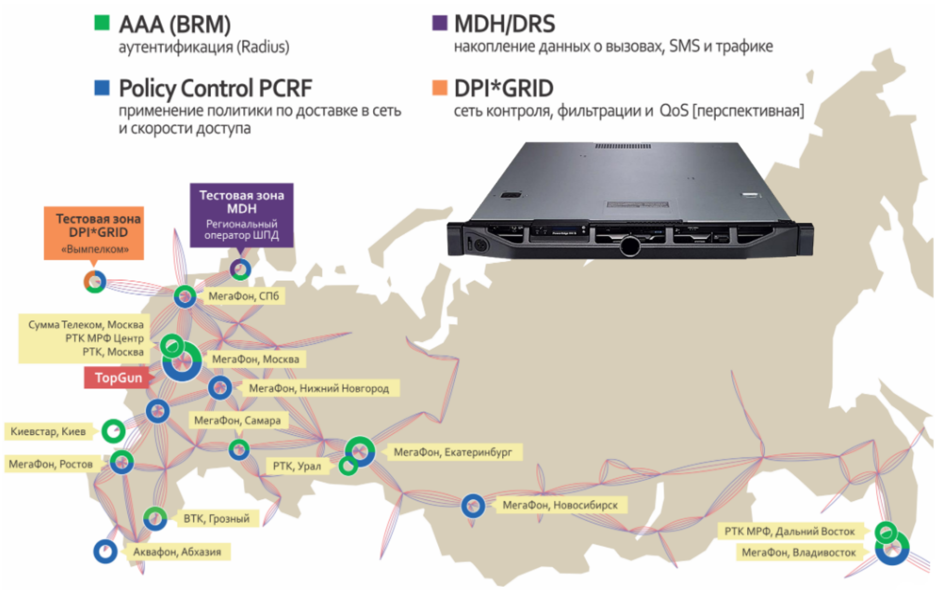
As a related document, this first release contains a publically available slide show presentation given by Валерий Сысик (Valery Syssik, Director of Development) from PETER-SERVICE at the Broadband Russia Forum in 2013. Titled *"National stacks of DPI / BigData / DataMining technologies and solutions for collection and analysis of information, as well as means of predicting social and business trends - the key to digital and financial sovereignty of the state and business in the XXI century"*, the presentation - which appears to already be publicly available on PETER-SERVICE's website - is not targeted at the usual telecom provider, but at a closed group of people from the ФСБ (FSB, Russian Federal Security Service), МВД (Interior ministry of Russia) and the *три ветви власти* ("three pillars of Power" - legislature, executive and judiciary).

The presentation was written just a few months after Edward Snowden disclosed the NSA mass surveillance program and its cooperation with private U.S. IT-corporations such as Google and access to a majority of all phone call records as well as Internet traffic in Russia, and in the description of the current experiences, it claims to have deployed technology for Deep Packet Inspection "with not just the headings of IP packets, but the contents of whole series". PETER-SERVICE is presented as a natural ally for intelligence agencies in "the most lucrative business [of] manipulating minds".

However, the core of the presentation is about a new product (2013) called *DPI*GRID* - a hardware solution for "Deep Packet Inspection" that comes literally as "black boxes" that are able to handle 10Gb/s traffic per unit. The national providers are aggregating Internet traffic in their infrastructure and are redirecting/duplicating the full stream to *DPI*GRID* units. The units inspect and analyse traffic (the presentation does not describe that process in much detail); the resulting metadata and extracted information are collected in a database for further investigation. A similar, yet smaller solution called MDH/DRS is available for regional providers who send aggregated IP traffic via a 10Gb/s connection to MDH for processing.



PETER-SERVICE advertises its experience in SORM technologies - especially DPI - and its ability to collect, manage and analyse "Big *a symbolic network alliance: operator - vendor - search engine - business - state organs."*



The above graphics shows the Internet backbone infrastructure in Russia and the nodes at various providers that run components of the proposed *DPI*GRID* system in different locations. The node *TopGun* most likely refers to a multi terabit DPI system developed by PETER-SERVICE.

About SORM

SORM is the technical infrastructure for surveillance in Russia. It dates back to 1995 and has evolved from SORM-1 (capturing telephone and mobile phone communications) and SORM-2 (interception of Internet traffic, 1999) to the current SORM-3. SORM now collects information from all forms of communication, providing long-term storage of all information and data on subscribers, including actual recordings and locations. In 2014, the system was expanded to include social media

Rights deemed Russia's SORM legislation in breach of the European Convention on Human Rights in 2015 (Zakharov v. Russia).

Media Partners

L'Repubblica - Italy

Mediapart - France

Top

WL Research Community - user contributed research based on documents published by WikiLeaks.

Tor is an encrypted anonymising network that makes it harder to intercept internet communications, or see where communications are coming from or going to.

Tails is a live operating system, that you can start on almost any computer from a DVD, USB stick, or SD card. It aims at preserving your privacy and anonymity.

The Courage Foundation is an international organisation that supports those who risk life or liberty to make significant contributions to the historical record.

Bitcoin uses peer-to-peer technology to operate with no central authority or banks; managing transactions and the issuing of bitcoins is carried out collectively by the network.