# Arquivos de espionagem da Rússia

Esta publicação dá continuidade à série Spy Files do WikiLeaks com comunicados sobre empresas de vigilância na Rússia.

Embora a vigilância do tráfego de comunicações seja um fenômeno global, o arcabouço legal e tecnológico de sua operação é diferente para cada país. As leis russas – especialmente a nova Lei Yarovaya – não fazem distinção entre Interceptação Legal e vigilância em massa por agências de inteligência estatais (SIAs) sem ordens judiciais. Os provedores de comunicação russos são obrigados pela lei russa a instalar os chamados componentes SORM (Система Оперативно-Розыскных Мероприятий) para vigilância, fornecidos pelo FSB às suas próprias custas. A infraestrutura SORM é desenvolvida e implantada na Rússia em estreita cooperação entre o FSB, o Ministério do Interior da Rússia e empresas de vigilância russas.



## Todos os lançamentos



## PETER-SERVICE

19 de setembro de 2017

Inglês | Russo

Hoje, 19 de setembro de 2017, o WikiLeaks inicia a publicação da série "Spy Files Russia" com documentos da empresa russa Петер-Сервис (PETER-SERVICE) . Esta publicação inclui 209 documentos (34 documentos base em diferentes versões) datados entre 2007 e 2015.

A PETER-SERVICE foi fundada em 1992 em São Petersburgo como fornecedora de soluções de faturamento e logo se tornou a principal fornecedora de software para o setor de telecomunicações móveis na Rússia. Hoje, conta com mais de 1.000 funcionários em diferentes localidades da Rússia e escritórios nas principais cidades da Rússia e da Ucrânia. As tecnologias desenvolvidas e implantadas pela PETER-SERVICE hoje vão muito além do processo clássico de faturamento e se estendem aos âmbitos da vigilância e do controle. Embora o cumprimento das rígidas leis de vigilância seja obrigatório na Rússia, em vez de ser obrigada a cumpri-las, a PETER-SERVICE parece estar buscando ativamente parcerias e oportunidades comerciais com o aparato de inteligência estatal .

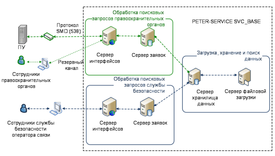
De fato, a PETER-SERVICE ocupa uma posição única como parceira de vigilância devido à notável visibilidade que seus produtos proporcionam aos dados de assinantes russos de operadoras de telefonia móvel, expondo à PETER-SERVICE metadados valiosos, incluindo registros telefônicos e de mensagens, identificadores de dispositivos (IMEI, endereços MAC), identificadores de rede (endereços IP), informações de torres de celular e muito mais. Esses metadados enriquecidos e agregados são, naturalmente, de interesse das autoridades russas, cujo acesso se tornou um componente central da arquitetura do sistema.

### Documentos vazados

- SISTEMA DE RETENÇÃO DE DADOS (PP, v5.1, ENU)
- ОСНОВНЫЕ ПОДСИСТЕМЫ (ЯДРО) СЕМЕЙСТВА ПРОДУКТОВ SPS (G3, v17.0, RUS)
- ОСНОВНЫЕ ПОДСИСТЕМЫ (ЯДРО) СЕМЕЙСТВА ПРОДУКТОВ SPS (L6, v5.0, RUS)
- ОСНОВНЫЕ ПОДСИСТЕМЫ (ЯДРО) СЕМЕЙСТВА ПРОДУКТОВ SPS (PP, v8.0, RUS)
- ОСНОВНЫЕ ПОДСИСТЕМЫ (ЯДРО) СЕМЕЙСТВА ПРОДУКТОВ SPS (GLOSS, v6.0, RUS)

Ver mais

### Componentes selecionados do software PETER-SERVICE




A arquitetura base do software do PETER-SERVICE ( SVC_BASE ) inclui componentes para retenção de dados (DRS [en] , [ru] ), armazenamento de longo prazo em *SORM* (SSP, Service СП-ПУ) , análise de tráfego IP (Traffic Data Mart, TDM) e interfaces (adaptadores) para agências estaduais acessarem os arquivos.

#### Mart de Dados de Tráfego (TDM)

O Traffic Data Mart é um sistema que registra e monitora o *tráfego* IP de todos os dispositivos móveis registrados na operadora. Ele mantém uma lista de nomes de domínio categorizados que abrangem todas as áreas de interesse do estado. Essas categorias incluem sites em lista negra, sites criminosos, blogs, webmail, armas, botnets, narcóticos, apostas, agressões, racismo, terrorismo e muito mais. Com base nas informações coletadas, o sistema permite a criação de relatórios para os dispositivos dos assinantes (identificados por IMEI/TAC, marca, modelo) para um intervalo de tempo especificado: principais categorias por volume, principais sites por volume, principais sites por tempo gasto, uso de protocolo (navegação, e-mail, telefonia, bittorrent) e distribuição de tráfego/tempo.

#### Sistema de Retenção de Dados (DRS)

O sistema de retenção de dados é um componente obrigatório para as operadoras por lei; ele armazena todos os (metadados de comunicação localmente por três anos. As autoridades de inteligência estaduais utilizam o adaptador de Protocolo 538 integrado ao DRS para acessar as informações armazenadas . De acordo com a PETER-SERVICE, sua solução DRS pode processar 500 milhões de conexões por dia em um único cluster. O tempo médio de busca de registros relacionados a assinantes em um único dia é de dez segundos.

#### Serviço СП-ПУ

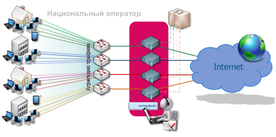
No *SORM*, as funções de monitoramento de chamadas concentram-se em pontos de controle (*пунктах управления, ПУ*) conectados às operadoras de rede. O Serviço СП-ПУ é uma interface de troca de dados baseada em HTTPS entre componentes em SVC_BASE/DRS e *SORM* . A interface recebe solicitações de busca de autoridades de inteligência estaduais e entrega os resultados ao iniciador. As solicitações de busca para interceptações legais (com base em uma ordem judicial) são processadas pela operadora no mesmo sistema.

### Produtos de inspeção profunda de pacotes

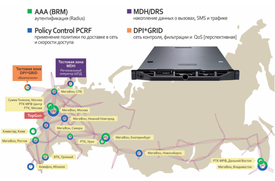
Como um documento relacionado, este primeiro lançamento contém uma apresentação de slides disponível publicamente feita por Валерий Сысюк (Valery Syssik, Diretor de Desenvolvimento) da PETER-SERVICE no Fórum de Banda Larga da Rússia em 2013. Intitulada *"Pilhas nacionais de tecnologias e soluções de DPI/BigData/DataMining para coleta e análise de informações, bem como meios de prever tendências sociais e empresariais - a chave para a soberania digital e financeira do estado e das empresas no século XXI"* , a apresentação - que parece já estar disponível publicamente no site da PETER-SERVICE - não é direcionada ao provedor de telecomunicações usual, mas a um grupo fechado de pessoas do ФСБ (FSB, Serviço Federal de Segurança Russo), МВД (Ministério do Interior da Rússia) e *трех ветвей власти* ("três pilares do poder" - legislativo, executivo e judiciário).

A apresentação foi escrita poucos meses após Edward Snowden revelar o programa de vigilância em massa da NSA e sua cooperação com empresas privadas de TI dos EUA, como Google e Facebook. Baseando-se especificamente no programa Prism da NSA, a apresentação propõe que autoridades policiais, serviços de inteligência e outras partes interessadas se unam a uma aliança para estabelecer operações equivalentes de mineração de dados na Rússia. A PETER-SERVICE afirma já ter acesso à maioria de todos os registros de chamadas telefônicas, bem como ao tráfego de internet na Rússia, e, na descrição das experiências atuais, afirma ter implantado tecnologia para Inspeção Profunda de Pacotes "não apenas com os títulos dos pacotes IP, mas com o conteúdo de séries inteiras". A PETER-SERVICE é apresentada como uma aliada natural das agências de inteligência no "negócio mais lucrativo de manipular mentes".

No entanto, o cerne da apresentação é sobre um novo produto (2013) chamado *DPI*GRID* – uma solução de hardware para "Inspeção Profunda de Pacotes" que vem literalmente como "caixas pretas" capazes de lidar com tráfego de 10 Gb/s por unidade. Os provedores nacionais estão agregando tráfego de internet em sua infraestrutura e redirecionando/duplicando o fluxo completo para unidades *DPI*GRID* . As unidades inspecionam e analisam o tráfego (a apresentação não descreve esse processo em muitos detalhes); os metadados resultantes e as informações extraídas são coletados em um banco de dados para investigação posterior. Uma solução semelhante, porém menor, chamada MDH/DRS, está disponível para provedores regionais que enviam tráfego IP agregado por meio de uma conexão de 10 Gb/s para o MDH para processamento.




A PETER-SERVICE divulga sua experiência em tecnologias SORM – especialmente DPI – e sua capacidade de *coletar, gerenciar e analisar* "Big Data" para fins comerciais e de inteligência. *"De soluções de DPI para SORM à publicidade contextual, temos a experiência e a solução. Oferecemos a coordenação de uma solução nacional escalável para o controle da rede digital. Buscamos uma cooperação eficaz dentro de uma aliança de rede simbólica: operadora – fornecedora – mecanismo de busca – empresa – órgãos estatais."*




O gráfico acima mostra a infraestrutura de backbone da Internet na Rússia e os nós em vários provedores que executam componentes do sistema *DPI*GRID* proposto em diferentes locais. O nó *TopGun* provavelmente se refere a um sistema DPI multiterabit desenvolvido pela PETER-SERVICE .

### Sobre a SORM

SORM é a infraestrutura técnica para vigilância na Rússia. Ela remonta a 1995 e evoluiu do SORM-1 (captura de comunicações telefônicas e celulares) e SORM-2 (interceptação de tráfego de internet, 1999) para o atual SORM-3. O SORM agora coleta informações de todas as formas de comunicação, fornecendo armazenamento de longo prazo de todas as informações e dados sobre assinantes, incluindo gravações e localizações reais. Em 2014, o sistema foi expandido para incluir plataformas de mídia social, e o Ministério das Comunicações ordenou que as empresas instalassem novos equipamentos com capacidade de Inspeção Profunda de Pacotes (DPI). Em 2016, o SORM-3 adicionou regulamentações confidenciais adicionais que se aplicam a todos os provedores de serviços de internet na Rússia. O Tribunal Europeu de Direitos Humanos considerou a legislação SORM da Rússia uma violação da Convenção Europeia de Direitos Humanos em 2015 (Zakharov v. Rússia).

### Parceiros de mídia

L'Repubblica - Itália

Mediapart - França