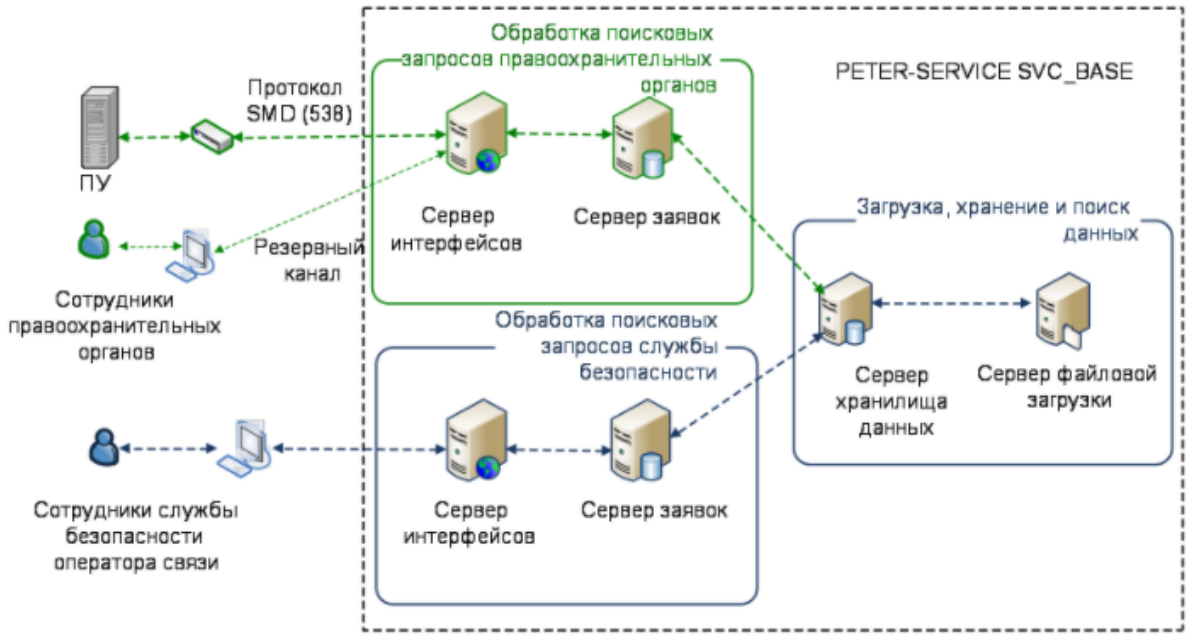
Wikileaks releases documents it claims detail Russia mass surveillance apparatus which copies the Cisco and Google USA Version

Posted by Natasha Lomas (@riptari)

-

Next Story



Wikileaks has released a new cache of documents which it claims detail surveillance apparatus used by the Russian state to spy on Internet and mobile users. It's the first time the organization has leaked (what it claims is) material directly pertaining to the Russian state.

As ever, nothing is straightforward when it comes to Wikileaks. And founder Julian Assange continues to face charges that his 'radical transparency' organization is a front for Kremlin agents (charges that stepped up after Wikileaks released a massive trove of hacked emails from the DNC last year at a key moment in the U.S. presidential election).

So it's entirely possible Wikileaks/Assange is here trying to deflect from such charges by finally dumping something on Russia.

Safe to say the Twitter arguments are already breaking out (e.g. see this tweet comment thread).

And it's not possible at this point to verify the veracity and/or value of the documents Wikileaks is releasing here.

Spy Files Russia

Writing a summary of the cache of mostly Russian-language documents, Wikileaks claims they show how a long-established Russian company which supplies software to telcos is also installing infrastructure, under state mandate, that enables Russian state agencies to tap into, search and spy on citizens' digital activity — suggesting a similar state-funded mass surveillance program to the one utilized by the U.S.'s NSA or by GCHQ in the U.K. (both of which were detailed in the 2013 Snowden disclosures).

> RELEASE: Spy Files #Russia https://t.co/CJMQVrNXef #SORM #FSB pic.twitter.com/QZPKY0HEWx
>
> — WikiLeaks (@wikileaks) September 19, 2017

The documents which Wikileaks has published (there are just 34 "base documents" in this leak) relate to a St. Petersburg-based company, called Peter-Service, which it claims is a contractor for Russian state surveillance. The company was set up in 1992 to provide billing solutions before going on to become a major supplier of software to the mobile telecoms industry.

Wikileaks writes:

> 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.

One of Wikileaks' initially stated media partners for the release, the Italian newspaper La Repubblica, (which has since been removed from the media partners' list and replaced with a different Italian publication's name — so, er, working with Assange must surely be a *lol* a minute…) reports that the documents cover "an extended timespan from 2007 to June 2015", and describes the contents as "extremely technical".

It also has a few caveats, noting the documents do not mention Russia's spy agency, the FSB, but rather "speak only of state agencies", a formula it asserts "certainly includes law enforcement, who use metadata for legal interception".

It also says the documents do “not clarify what other state apparatus accesses those data through the solution of the St. Petersburg company”.

Wikileaks says that under Russia law operators must maintain a Data Retention System (DRS), which can store data for up to three years. La Repubblica reports that Peter-Service’s DRS stores telephone traffic data and “allows Russian state agencies to query the database of all stored data in search of information” — which it specifies can include calls made by a certain telephone company’s customer; payment systems used; the cell phone number to which a user is calling.

“The manuals published by WikiLeaks contain the images of interfaces that allow you to search within these huge data fields, so access is simple and intuitive,” it adds.

According to Wikileaks, Peter-Service’s DRS solution can handle 500,000,000 connections per day in one cluster. While the claimed average search time for subscriber related-records from a single day is ten seconds. “State intelligence authorities use the *Protocol 538* adapter built into the DRS to access stored information,” it adds.

Peter-Service has also apparently developed a tool called TDM (Traffic Data Mart) — which allows the database to be queried to determine “where users’ data traffic is stored in order to understand visited sites, forums, social media”, as well as how much time is spent on a certain site and the electronic device used to access it.

Wikileaks describes TDM as “a system that records and monitors IP traffic for all mobile devices registered with the operator”, and says 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,” it adds.

Wikileaks points to a 2013 Peter-Service slideshow presentation (it says this also appears to be publicly available on the company’s website), which it claims is targeted not at telco customers but at state entities such as Russia’s FSB and Interior Ministry (despite this document apparently being in the public domain) — in which the company focuses on a new product, called *DPI*GRID*; which it says is a hardware device for Deep Packet Inspection that takes the form of “black boxes” apparently 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,” writes Wikileaks. “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.”

Wikileaks also makes a point of noting that 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 Facebook”.

“Drawing specifically on the NSA Prism program, the presentation offers law enforcement, intelligence and other interested parties, to join an alliance in order to establish equivalent data-mining operations in Russia,” it adds — sticking its boot firmly back into U.S. government mass surveillance programs.