

'The Surkov Leaks' Reveal the Expected: Kremlin's Guiding Hand in Eastern Ukraine

October 26, 2016



Vladislav Surkov **Kremlin Press Service**

Hackers from the Ukrainian group Cyber Hunta claim to have hacked two email accounts belonging to Vladislav Surkov, the Kremlin's longtime grey cardinal and reportedly in charge of relations with Ukraine. If authentic, the leaked emails prove that the Kremlin was constantly in touch with rebels in eastern Ukraine throughout 2014 as the conflict there started to unravel.

According to the Cyber Hunta website, hackers obtained access to Surkov's personal email account via Russia's biggest search engine Yandex. Anton Gerashenko, advisor to Ukraine's Interior Ministry, claimed in a Facebook post that the Yandex emails were authentic. "The hacking into Vladislav Surkov's email is genuine. The documents leaked by Cyber Hunta are real," Gerashenko wrote on Monday.

However, cybersecurity analysts note that the emails and documents from the Yandex account were published in the form of screenshots and PDFs – formats that can be easily forged. At the same time, emails from the office account seem to be authentic.

“With the publication of nearly 1gb of Outlook data files (.PST) (including the inbox, outbox, drafts, deleted email, spam, etc.), it is fairly clear that the emails are authentic. It is quite easy to fake screenshots, PDF documents, and other files, but faking email inboxes is quite difficult. Within the email files (.MSG files, in this instance) is header information, which shows us the “history” of each email — where it originated, which servers it moved through, and so on,” reads the blog of the Digital Forensic Research lab.

Most of the emails from Surkov's office account contain briefings from his assistants on situations in Abkhazia, South Ossetia, Ukraine and Moldova – areas Surkov was reportedly in charge of.

Some emails, however, include bits of information showing that Surkov was deeply involved in the situation in eastern Ukraine in 2014 and remained in contact with the rebels' leaders. For example, he received a list of casualties in Donbass from a high-ranking separatist official, expense reports for a government office in Donetsk, and requests for edits on a “letter from the Donbass residents” to Ukrainian authorities, calling to cease all military activities in the region. The document would later surface in the pro-Kremlin media as authentic.

“The Surkov Leaks, as they have been called on Twitter since their release, show us a picture of the conflict in Eastern Ukraine that we have long suspected: the Kremlin had a guiding hand in orchestrating and funding the supposedly local and independent government,” the Digital Forensic Research Lab wrote.

Surkov himself hasn't yet commented on the leak.

The Kremlin spokesman Dmitry Peskov at first neither confirmed nor denied the fact that the hacking took place. “I've known Surkov for more than 10 years, and things are being attributed to him all the time by either Russian hackers or the ones abroad. He is a very talented man, so everyone, naturally, tries to attribute things to him. Often it is not true,” Peskov was quoted by the Interfax news agency as saying. The Kremlin spokesman later said that Surkov “doesn't use email at all” and denied the hacking took place. “Someone must have really sweated over forging this,” Peskov was quoted by Interfax as saying.

Original url:

<https://www.themoscowtimes.com/2016/10/26/the-surkov-leaks-reveal-the-expected-kremlins-guiding-hand-in-eastern-ukraine-a55879>