The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

An American Cover Story for Russia's Undercover Hackers

An unprecedented spy saga plays out at the heart of Russia's intelligence community.

By Eva Hartog and Mikhail Fishman

February 01, 2017

Olya Khaletskaya

Even for a spy thriller, the plot is borderline fantastical.

Two top FSB cyber crime fighters hunt down a group of hackers behind the personal data leaks of some of the Kremlin's most powerful and mighty.

Rather than arrest them, they take over the organization and put it to their own use. Several months on, the chief cyber detective is outed by his own colleagues at an FSB meeting and escorted out of the room with a bag over his head.

Since the nationalist Tsargrad outlet first broke the story on Jan. 25, more murky details have emerged every day.

Citing anonymous leaks from within the security apparatus, the Russian press reports the officials and two others have been accused of colluding with American intelligence services to expose Russian hacking there. The trail leads from Lubyanka to Bangkok and the United States, and stars characters with names like the Mad Hatter and Humpty Dumpty.

Real information is scant, but one thing is sure: the four accused are being held at Moscow's notorious Lefortovo prison. Both FSB officials refused to talk to Kogershin Sagiyeva, a member of the independent prison watchdog ONK. But she got a glimpse of them.

"I was amazed by how young they looked," she told The Moscow Times, "not what you'd expect from high-ranking law enforcement officials."

Whether or not the men are double agents or victims of an internal power struggle, a purge is under-way and it is expanding like an oil spill.

The Art of Black PR

The story begins in 1990s St. Petersburg, where Vladimir Anikeyev started his career in journalism, according to the Rosbalt news agency. A mediocre writer, Anikeyev nonetheless excelled at "getting the required information."

Soon, Anikeyev shifted to doing "black PR." He cozied up to secretaries and insiders to collect incriminating evidence on officials and businessmen, known in Russia as *kompromat*. He would then either extort money from his victims or sell the information to rivals or media outlets, the report claims.

Joining forces with a number of hackers, he used phishing emails and set up fake Wi-Fi networks at venues he knew were popular with high-placed Kremlin officials, such as the GUM department store on Red Square. After gaining access to the victims' gadgets, the stolen content was stored on servers in Estonia, Thailand and Ukraine.

Anikeyev and his team took up aliases inspired by British author Lewis Carroll's *Through the Looking Glass*. Anikeyev became Lewis, his right hand was Alice and the group's press representatives went by Shaltai and Boltai (Russian for Humpty and Dumpty).

"That world of inside-out logic best describes Russian politics," Shaltai told the Apparat.ru news website during an encrypted chat interview several years ago, explaining their name choice.

The group organized anonymous bitcoin cyptocurrency auctions on their own website, offering leaked content to the highest bidder. One source who claimed to have participated in the auctions told The Moscow Times that an average lot would sell for up to $30,000. Some hacks, however, attracted bids as high as $200,000, the source added.

FSB Ties

Shaltai Boltai,⊠ as the group became known, first made itself known to the general public in 2013, when it published an⊠ online transcript of President Vladimir Putin's traditional New Year's ⊠Eve speech, hours before it hit the airwaves.

In⊠ 2014, the group hacked Prime Minister Dmitry Medvedev's Twitter account and ⊠sent out tweets announcing his resignation "out of shame for this ⊠government's actions" and criticizing the annexation of Crimea. The group also published the private email correspondence of a number of other high officials and businessmen.

According⊠ to Rosbalt, the head of the FSB's cyber crime investigation unit ⊠(TsIB), Sergei Mikhailov, and his deputy, Dmitry Dokuchayev, uncovered ⊠Shaltai Boltai's real identities in 2016. Instead of dissolving the ⊠group, however, they took control.

But some argue the nature ⊠of the information being leaked proved the group had ties to the FSB from the outset.

A Moscow Times source who claims to have been blackmailed by Shaltai Boltai, ⊠insists the information that Shaltai gathered on him "could have been obtained only by surveillance and operative action, not just hacking." This would mean that Mikhailov ⊠could have been involved in Shaltai's activities from its founding, the source said.

In⊠ any case, in autumn 2016, the group got hold of thousands of messages ⊠from the official email account of Vladislav Surkov, the coordinator of ⊠Russia's Ukraine policy, and shared it with Ukrainian news websites.

⊠By⊠ targeting Surkov, the group might have gone a step too far. In October, Anikeyev was detained after crossing the border into Russia. The ⊠arrest was the culmination of an operation that took at least a few ⊠months and involved several exchanges with the group, according to a ⊠source close to the top-level state authorities. It was not the FSB that arrested Mikhailov, as claimed by most Russian media, but the Federal Security Guard service (FSO), he says.

Within⊠ Russia's security apparatus, the FSO is the FSB's main competitor. If ⊠the sting operation was under FSO control, it would suggest the ⊠detentions were part of an internal power struggle between security ⊠bodies.

Following his arrest, Anikeyev allegedly started cooperating with the ⊠authorities and revealed the supposed involvement of the FSB's own cyber⊠ crime chief, Mikhailov, Russian media reports.

A Cover-Up

Mikhailov and deputy Dokuchayev were detained in several months later, in December, and charged with treason. It is unclear, however, what the men stand accused of.

On⊠ Jan. 31, the Interfax news agency connected the treason charges to ⊠American accusations of Russian hacking ahead of the U.S. presidential ⊠elections. It is as close to an

official statement as can be expected in Russia.

American intelligence agencies have expressed "high confidence" that the cyber attacks emanated from Moscow. Some now think Mikhailov and his deputy might have funnelled confidential information to the U.S. on Russian hacks of the Arizona and Illinois voter registration databases. To Steven L. Hall, a former CIA head of Russian operations, the connection between the Russian hacking scandal and the recent arrests seems "reasonable."

"Certainly U.S. intelligence would have loved to talk to Mikhailov," Hall told The Moscow Times. "But how that could have happened is a complicated question."

However, according to two Moscow Times sources, the treason charges and the men's supposed link to America are likely a cover story. Politically, the loss of Shaltai Boltai is a big blow to the FSB's reputation. The U.S. connection makes it easier to explain to an external audience what is, in fact, an internal power struggle, they said.

Rabbit Hole

The scandal shows no sign of ending. So far, according to several media reports, six people have been detained, including the FSB officials, Anikeyev and Ruslan Stoyanov, the head of investigations at Russia's prominent Kaspersky Lab cybersecurity company.

Meanwhile, at the Lefortovo prison, only Stoyanov agreed to talk with prison monitor Sagiyeva, and only to confirm the date of his detention. Sagiyeva also twice tried to visit Anikeyev, but was told both times he was away at a meeting with investigators.

"Something's going on," she told The Moscow Times. "I doubt he is even there."

As in Shaltai Boltai's description of Russian politics, nothing in this case is what it seems.