Leaked chats show alleged Russian spy seeking hacking tools

August 1 2018, by Raphael Satter And Matthew Bodner

This Tuesday, July 31, 2018 photo shows the entrance of the building of the Russian military intelligence service, named in Robert Mueller's July 13 indictment, as home to GRU Unit 26165 in Moscow, Russia. The leak of an alleged Russian hacker's conversations with a security researcher shows more about the shadowy group of 12 Russian spies indicted by the FBI last month for targeting the 2016 U.S. election. (AP Photo/Alexander Zemlianichenko)

Six years ago, a Russian-speaking cybersecurity researcher received an unsolicited email from Kate S. Milton.

Milton claimed to work for the Moscow-based anti-virus firm Kaspersky. In an exchange that began in halting English and quickly switched to Russian, Milton said she was impressed by the researcher's work on exploits—the digital lock picks used by hackers to break into vulnerable systems—and wanted to be copied in on any new ones that the researcher came across.

"You almost always have all the top-end exploits," Milton said, after complimenting the researcher about a post to her website, where she often dissected malicious software.

"So that our contact isn't one-sided, I'd offer you my help analyzing malicious viruses, and as I get new samples I'll share," Milton continued. "What do you think?"

The researcher—who works as a security engineer and runs the malware-sharing site on the side—always had a pretty good idea that Milton wasn't who she said she was. Last month, she got confirmation via an FBI indictment.

The indictment , made public on July 13, lifted the lid on the Russian hacking operation that targeted the 2016 U.S. presidential election. It identified "Kate S. Milton" as an alias for military intelligence officer Ivan Yermakov, one of 12 Russian spies accused of breaking into the Democratic National Committee and publishing its emails in an attempt to influence the 2016 election.

The researcher, who gave her exchanges with Milton to The Associated Press on condition of anonymity, said she wasn't pleased to learn she had been corresponding with an alleged Russian spy. But she wasn't particularly surprised either.

"This area of research is a magnet for suspicious people," she said.

The researcher and Milton engaged in a handful of conversations between April 2011 and March 2012. But even their sparse exchanges, along with a few digital breadcrumbs left behind by Yermakov and his colleagues, offer insight into the men behind the keyboards at Russia's Main Intelligence Directorate, or GRU.

This May 14, 2018, photo shows a poster inside the Russian military base in Moscow named in Robert Mueller's July 13 indictment against 12 Russians spies.

Leaked of email conversations between a security researcher and one of the people in the indictment, Ivan Yermakov, who's Unit 26165 was located at the base, reveal new insights about the shadowy group of the spies accused of breaking into the Democratic National Committee during the 2016 election. (AP Photo)

—

It isn't unusual for messages like Milton's to come in out of the blue, especially in the relatively small world of independent malware analysts.

"There was nothing particularly unusual in her approach," the researcher said. "I had very similar interactions with amateur and professional researchers from different countries."

The pair corresponded for a while. Milton shared a piece of malicious code at one point and sent over a hacking-related YouTube video at another, but contact fizzled out after a few months.

Then, the following year, Milton got back in touch.

"It's been all work, work, work," Milton said by way of apology, before quickly getting to the point. She needed new lock picks.

"I know that you can help," she wrote. "I'm working on a new project and I really need contacts that can provide information or have contacts with people who have new exploits. I am willing to pay for them."

In particular, Milton said she wanted information on a recently disclosed vulnerability codenamed CVE-2012-0002 - a critical Microsoft flaw that could allow hackers to remotely compromise some Windows computers.

Milton had heard that someone had already cobbled together a working exploit.

"I'd like to get it," she said.

In this file photo taken on Saturday, July 14, 2018, a man walks past the building of the Russian military intelligence service in Moscow, Russia. The leak of an alleged Russian hacker's conversations with a security researcher shows more about the shadowy group of 12 Russian spies indicted by the FBI last month for targeting the 2016 U.S. election. (AP Photo/Pavel Golovkin, File)

The researcher demurred. The trade in exploits—for use by spies, cops, surveillance companies or criminals—can be a seedy one.

"I usually steer clear from any wannabe buyers and sellers," she told the AP.

She politely declined - and never heard from Milton again.

—

Milton's Twitter account—whose profile photo features "Lost" star Evangeline Lilly—is long dormant. The last few messages carry urgent, awkwardly worded appeals for exploits or tips about vulnerabilities.

"Help me find detailed description CVE-2011-0978," one message reads, referring to a bug in PHP, a coding language often used for websites. "Need a work exploit," the message continues, ending with a smiley face.

It isn't clear whether Yermakov was working for the GRU when he first masqueraded as Kate S. Milton. Milton's Twitter silence—starting in 2011—and the reference to a "new project" in 2012 might hint at a new job.

In any case, Yermakov wasn't working for the anti-virus firm Kaspersky—not then and not ever, the company said in a statement.

"We don't know why he allegedly presented himself as an employee," the statement said.

In this photo taken on Tuesday, July 31, 2018, a view shows a building of the Russian military intelligence service, located at 22 Kirova Street, Khimki, which was named in an indictment announced by a U.S. federal grand jury as part of a probe into alleged Russian involvement in the 2016 U.S. presidential election, in Khimki outside Moscow, Russia. The leak of an alleged Russian hacker's conversations with a security researcher shows more about the shadowy group of 12 Russian spies indicted by the FBI last month for targeting the 2016 U.S. election. (AP Photo/Alexander Zemlianichenko)

Messages sent by the AP to Kate S. Milton's Gmail account were not returned.

The exchanges between Milton (Yermakov) and the researcher could be read in different ways.

They might show that the GRU was trying to cultivate people in the information security community with an eye toward getting the latest exploits as soon as possible, said Cosimo Mortola, a threat intelligence analyst at the cybersecurity company FireEye.

It's also possible that Yermakov might have initially worked as an independent hacker, hustling for spy tools before being hired by Russian military intelligence—a theory that makes sense to defense and foreign policy analyst Pavel Felgenhauer.

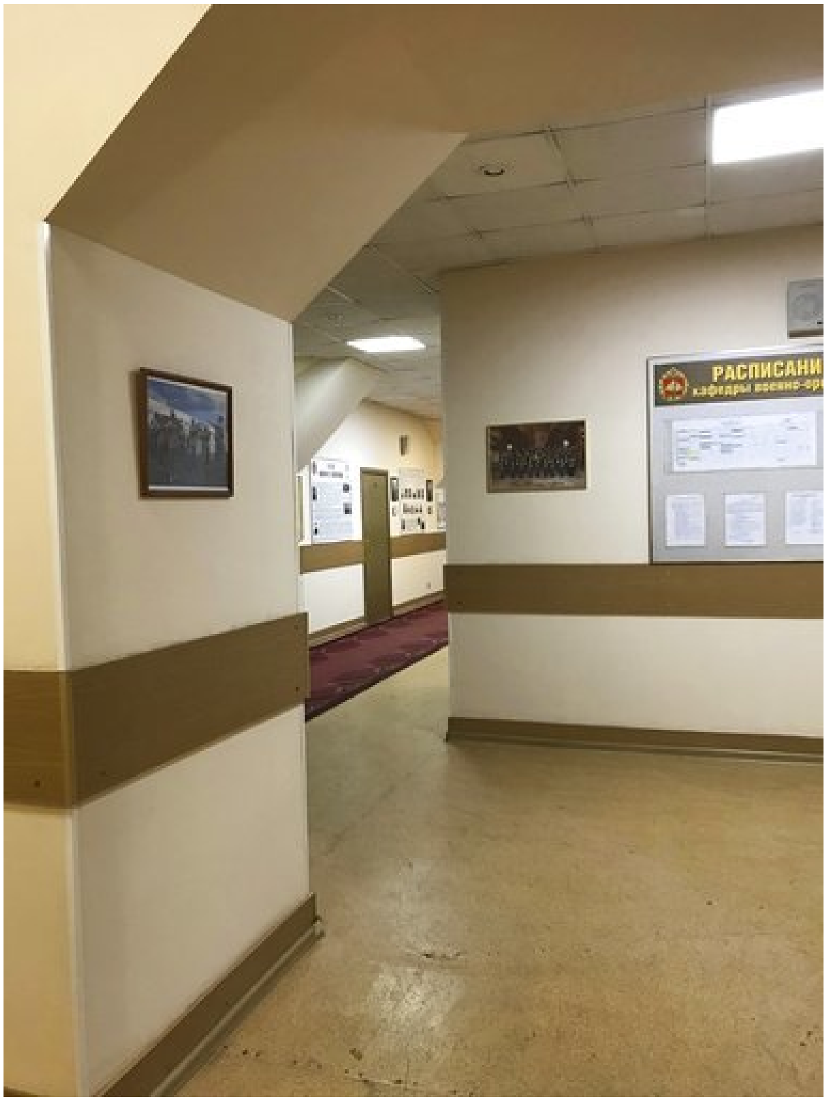
"For cyber, you have to hire boys that understand computers and everything the old spies at the GRU don't understand," Felgenhauer said. "You find a good hacker, you recruit him and give him some training and a rank—a lieutenant or something—and then he will do the same stuff."

___

The leak of Milton's conversations shows how the glare of publicity is revealing elements of the hackers' methods—and perhaps even hints about their private lives.

It's possible, for example, that Yermakov and many of his colleagues commute to work through the arched entrance to Komsomolsky 22, a military base in the heart of Moscow that serves as home to the alleged hacker's Unit 26165. Photos shot from inside show it's a well-kept facility, with a czarist-era facade, manicured lawns, flower beds and shady trees in a central courtyard.

The AP and others have tried to trace the men's digital lives, finding references to some of those indicted by the FBI in academic papers on computing and mathematics, on Russian cybersecurity conference attendee lists or—in the case of Cpt. Nikolay Kozachek, nicknamed "kazak"—written into the malicious code created by Fancy Bear, the nickname long applied to the hacking squad before their identities were allegedly revealed by the FBI.



This photo taken on Monday, May 14, 2018, a view inside the Russian military base at 20, Komsomolsky Prospect, named in Robert Mueller's July 13 indictment. The leak of an alleged Russian hacker's conversations with a security researcher shows how the glare of publicity is the shadowy group indicted by the FBI into focus. (AP Photo)

One of Kozachek's other nicknames also appears on a website that allowed users to mine tokens for new weapons to use in the first-person shooter videogame "Counter Strike: Global Offensive"—providing a flavor of the hackers' extracurricular interests.

The AP has also uncovered several social media profiles tied to another of Yermakov's indicted colleagues—Lt. Aleksey Lukashev, allegedly the man behind the successful phishing of the email account belonging to Hillary Clinton's campaign chairman, John Podesta.

Lukashev operated a Twitter account under the alias "Den Katenberg," according to an analysis of the indictment as well as data supplied by the cybersecurity firm Secureworks and Twitter's "Find My Friends" feature.

A tipster using the Russian facial recognition search engine FindFace recently pointed the AP to a VKontatke account that, while using a different name, appears active and features photos of the same young, Slavic-looking man.

Many of his posts and his friends appear to originate from a district outside Moscow known as Voskresensky. The photos show him cross-country skiing at night, wading in emerald waters somewhere warm and visiting Yaroslavl, an ancient city northwest of Moscow. One video appeared to show Russia's 2017 Spasskaya Tower Festival, a military music festival popular with officers.

The AP could not establish with certainty that the man on the VKontatke account is Lukashev. Several people listed as friends either declined to comment when approached by the AP or said Lukashev's name was unknown to them.

Shortly thereafter, the profile's owner locked down his account, making his vacation snaps invisible to outsiders.

More information: The exchanges between the cybersecurity researcher and Kate S. Milton are available here: www.documentcloud.org/document … -S-Milton-Chats.html

Citation: Leaked chats show alleged Russian spy seeking hacking tools (2018, August 1) retrieved 9 April 2024 from https://phys.org/news/2018-08-leaked-chats-alleged-russian-spy.html