

Taiwan Opposition Hacked as China's Cyberspies Step Up Attacks

Tim Culpan David Tweed
tculpan DavidTweed

December 20, 2015 — 2:01 PM PST Updated on December 20, 2015 — 5:04 PM PST



Buildings stand illuminated at night in Taipei, Taiwan.

Photographer: Tomohiro Ohsumi/Bloomberg

- ▶ FireEye says media targeted by China-based cyberhackers
- ▶ Gmail accounts of former U.S. diplomat, DPP staff were targets

Chinese hackers have attacked Taiwanese targets including local news organizations and the opposition Democratic Progressive Party in a bid to get information about policies and speeches ahead of presidential and legislative elections next month.

An attack on the unnamed media outlets came in the form of phishing e-mails with the subject line "DPP's Contact Information Update," according to research by security company FireEye Inc., which identified a Chinese state-backed group called APT16 as carrying out attacks. Hackers also infiltrated e-mails of party staff, changing security protocols and writing messages spoofing the account holders in what may have been an attempt to deliver malicious code, according to one of the victims.

Taiwan goes to the [polls](#) Jan. 16 and opinion surveys show the DPP is likely to win a legislative majority, with its leader Tsai Ing-wen securing the presidency after eight years of nationalist Kuomintang rule. China, which considers Taiwan to be one of its provinces, is wary of the DPP's views on Taiwan independence and advocacy of more caution in its relationship with the mainland.

As well as not wanting the DPP in power, China may want to understand the party better so as to undermine them with access to non-public information, FireEye Principal Threat Intelligence Analyst Jordan Berry said by phone. "There's a lot of people in China who want and need information for their own intelligence purposes."

Other Targets

China's Ministry of Foreign Affairs didn't reply to a faxed request for comment.

FireEye, based in California, provides malware and network-threat protection systems. After its Mandiant division alleged in February 2013 that China's military may be behind a group that hacked at least 141 companies worldwide since 2006, the U.S. issued indictments against five military officials who were purported to be members of that group.

Another target in Taiwan appears to be former U.S. diplomat to Taiwan William Stanton who said he's received multiple warnings from Google Inc. that his Gmail account may be targeted by government hackers.

"If you were directed to this page from a warning displayed above your Gmail inbox, we believe that state-sponsored attackers may be attempting to compromise your account or computer," the warning read without identifying the country. "It's likely that you received emails containing malicious attachments, links to malicious software downloads, or links to fake websites that are designed to steal your passwords or other personal information."

Increased Frequency

Stanton, who was director of the American Institute in Taiwan from 2009 to 2012 in a position akin to ambassador, told Bloomberg News he believes he's being targeted because of his former role as well as his current position as Director of Taiwan's National Tsing Hua University Center for Asia Policy.

While the DPP has been under attack for months, the frequency has picked up in the past few weeks, said Ketty Chen, deputy director of international affairs at the DPP, whose own account was compromised.

Chen was among as many as 50 DPP staff targeted by hackers and was alerted when she noticed inconsistencies in the writing style of a colleague in internal correspondence.

Suspicious E-mails

"There were fake e-mails that looked like they came from her," Chen said. "When I read it, the style was not how she would talk so I called to ask if she really sent it, and she hadn't."

Chen received e-mails purporting to come from Tsai's speechwriter and another from a member of the DPP's cross-strait policy team. In each case the e-mail asked the recipient to open an attachment purporting to be a draft document. Hackers typically send e-mails to targets hoping they'll open attachments loaded with malware that infiltrate their computers, providing links to those of colleagues' computers and contacts.

With concerns over security of their work accounts, some DPP staff switched to Gmail, Chen said. Chen's Gmail account was compromised when hackers turned off the two-step identification verification process by deleting her mobile number, and adding a forwarding address so that all incoming e-mails went to an external Gmail account.

The allegations come weeks after state-run Xinhua News Agency reported that an investigation into an alleged theft of data from the U.S. Office of Personnel Management had shown the attack was carried out by criminals, rather than being state-sponsored as previously suspected by the U.S. government. Cyberspace must not become a "battlefield" between states, President Xi Jinping said at an Internet conference Wednesday in Wuzhen, and he called for greater cooperation on punishing cyber-attacks and fighting terrorism.

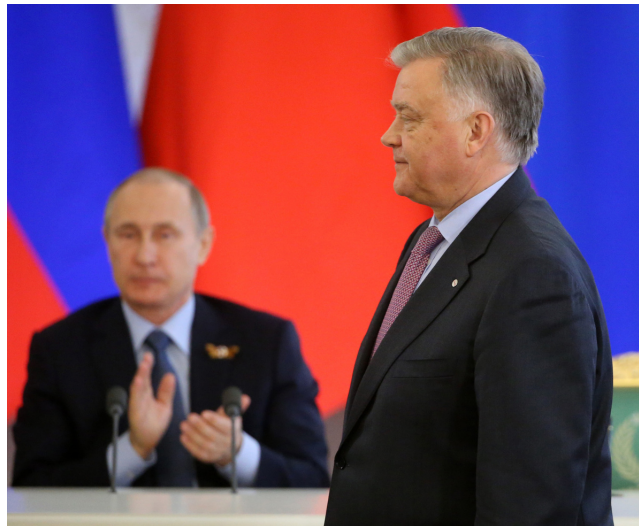
Before it's here, it's on the Bloomberg Terminal.

• Taiwan • China • FireEye Inc

A Fallen Russia Oligarch Sends Warning to Rest of Putin Insiders

Irina Reznik

January 12, 2016 — 6:00 PM PST



Putin and Yakunin. Photographer: Sasha Mordovets/Getty Images

- ▶ Ex-rail boss says Russia has no ruling elite, just Putin
- ▶ Putin's inner circle will 'continue to rotate,' Yakunin Says

He was one of the most powerful men in Russia for a decade, an old pal of the president who oversaw a million workers and a rail network spanning 11 time zones.

But then Vladimir Yakunin was suddenly out, ending a career that included a stint as an intelligence officer at the United Nations in New York during the Cold War. Now Yakunin, 67, has some parting

<http://www.bloomberg.com/news/articles/2015-12-20/taiwan-opposition-hacked-as-china-s-cyberspies-step-up-attacks-iif2vmh1>

advice for the remaining members of what he dismissed as Putin's "so-called inner circle": know your place.

"This circle will continue to rotate," Yakunin said in his private office in Moscow during a 90-minute interview. Putin has yet to form a stable "ruling class like Russia had during czarist times," the former head of state-owned Russian Railways JSC said.

The comments are a rare public admission from a longtime insider of the fragility of wealth and influence in the opaque and seemingly ironclad system of control Putin has built over 15 years. With that system under unprecedented pressure from plunging oil prices and international sanctions, any step Putin takes to maintain his grip on power reverberates far beyond Moscow.

Berezovsky Warning

Some insiders are making the mistake of viewing their property and privilege as inalienable rights, but everything they have hinges on Putin's shifting views of what's good for Russia, according to Yakunin. He offered two examples from the president's first term to illustrate the dangers of overreach.

"Remember what happened to Boris Berezovsky and Vladimir Gusinsky," he said, referring to two post-Soviet oligarchs who lost their fortunes trying to influence Putin's Kremlin the way they did Boris Yeltsin's.

Yakunin's departure from the rail monopoly in August was the biggest shakeup in years within "the new politburo," the highest authority under communism, and presages more to come, according to Olga Kryshтанovskaya, a sociologist who's tracked the rise of the security services under retired KGB Colonel Putin.

"Rough resignations" by Putin loyalists are rare and Yakunin's rejection of the customary senate seat as consolation is even more so, she said.

The U.S. blacklisted Yakunin in its initial round of sanctions over the Ukraine conflict in March 2014 for being both "a close confidant of Putin" and an influential government official; Russian Railways carries more than a billion passengers and a billion tons of cargo a year.

Dacha Buddies

Yakunin and other members of Putin's St. Petersburg clique in the 1990s, including his chief of staff and fellow former spy Sergei Ivanov, constitute "the Russian leadership's inner circle," the Treasury Department said at the time.

"Yakunin and Putin were also neighbors in the elite dacha community on the shore of Lake

Komsomolsk and they served as co-founders of the Ozero Dacha Cooperative in November 1996." it
<http://www.bloomberg.com/news/articles/2015-12-20/taiwan-opposition-hacked-as-china-s-cyberspies-step-up-attacks-iif2vmh1>

ROMSOMOLSK and they served as co-founders of the OZERO Dacha Cooperative in November 1990, it said.

Another Ozero founder, Yuri Kovalchuk, was also among the first 20 Russians sanctioned, as were three other St. Petersburg businessmen who became billionaires after Putin came to power -- Gennady Timchenko and the brothers Arkady and Boris Rotenberg.

The reasons Yakunin was kicked out of this exclusive club are disputed.

British Passport

He says publicly the decision to resign was his own and Putin approved it, but people familiar with the matter said the president felt betrayed when Yakunin's eldest son obtained citizenship from the U.K. when that country was penalizing Russia over Ukraine.

The Kremlin was aware of the issue and nobody objected, Yakunin said.

"My son has lived in the U.K. for five years and had the right to obtain citizenship," he said. "I made no secret of this from the country's leadership."

Putin's spokesman, Dmitry Peskov, declined to comment.

Kryshtanovskaya, the sociologist, said it may have just been a matter of mismanagement at Russian Railways. The company had become bloated, inefficient and plagued by accusations of corruption, so new leadership was needed, especially with the economy mired in a recession, she said.

Safeguarding Wealth

The man picked to replace Yakunin, Oleg Belozerov, is a 46-year-old logistics specialist and deputy transport minister from St. Petersburg who has longstanding ties to the Rotenbergs.

Evgeny Minchenko, who runs the International Institute for Political Expertise in Moscow, said Yakunin was simply outmaneuvered by more aggressive insiders whose business interests were being hampered by the rail monopoly.

Whatever the cause, Minchenko said one thing is indisputable: People close to Putin, who could extend his rule to a quarter century if he wins re-election in 2018, are increasingly focused on safeguarding their wealth and status to pass them on to their offspring.

Putin In-Law

Some are even joining Putin's family.

Kirill Shamalov, the son of Nikolay Shamalov, another co-founder of the dacha cooperative cited by the Treasury Department, married Putin's youngest daughter Katerina in 2013 and then became a tycoon in his own right, thanks mainly to a stake in a petrochemical company he acquired from Timchenko with financing from a state bank.

Still, nobody's position but Putin's will be secure until a governing elite like the one that existed before the Bolsheviks swept to power a century ago is fully formed, a process that may take decades, according to Yakunin.

"Trying to measure influence by proximity to political resources is a relic of the Soviet system," he said.

Before it's here, it's on the Bloomberg Terminal.

Read this next

▶ Kadyrov Calls Russian Political Opposition Enemies of the People

▶ Goldman's Bullish Rate-Cut Forecast for Russia Upended by Oil

▶ Ruble Set for Best Gain in Three Weeks as Citi Says Risks Remain

• Vladimir Ivanovich Yakunin • Russia

