Chinese Cyberspies Pivot To Russia In Wake Of Obama-Xi Pact

darkreading.com/endpoint/chinese-cyberspies-pivot-to-russia-in-wake-of-obama-xi-pact/d/d-id/1324242

Kelly Jackson Higgins February 9, 2016

Endpoint
3 MIN READ

ARTICLE
Kaspersky Lab has identified a massive uptick in cyber espionage in Russia by 'Chinese-speaking' APTs.

Kelly Jackson Higgins
Editor-in-Chief, Dark Reading
February 09, 2016

TENERIFE, SPAIN – Kaspersky Security Analyst Summit 2016 – Cyber espionage attacks by Chinese advanced persistent threat groups against Russian targets have increased by 300 percent in the past two months, according to a top security expert with Kaspersky Lab.

Costin Raiu, director of the global research and analysis team at Kaspersky Lab, says his firm's researchers witnessed a dramatic drop in Chinese-speaking APTs going after US and UK organizations' intellectual property in September after President Obama and Chinese president Xi Jinping came to a historic agreement not to conduct cyber spying attacks for

economic gain. Kaspersky Lab refrains from confirming the actual actors behind advanced groups such as nation-states, so it refers to these attackers as "Chinese-speaking" cyber espionage groups.

“Immediately after the signing of the agreement, there was silence” in attacks against the US, Raiu said in an interview with *Dark Reading*. “Then there were some small bits and pieces of random noise … but after that, they [Chinese-speaking APTs] completely went silent in the US and UK,” Raiu said, referring to Xi’s similar no-hack deal in October with Prime Minister Cameron in the UK.

Raiu said the cyber espionage groups appear to have shifted their focus to Russia and other former Soviet countries as new sources of intellectual property for economic gain in the wake of the Obama-Xi pact.

While the Obama-Xi agreement was applauded by the security and IT industries as a good first step, critics had expected China ultimately not to fully comply with the agreement. Those concerns appeared to come to fruition in October, when CrowdStrike reported spotting multiple Chinese APT groups attempting to steal business secrets from seven US companies in the technology and pharmaceutical industries the day after the Obama-Xi agreement. The Obama-Xi pact stops short of banning traditional espionage via hacking.

Kaspersky’s Raiu said his company has seen activity from Mirage, a Chinese-speaking APT group that traditionally has targeted ministries of foreign affairs, waging attacks in Russia. “Now they are super-active in Russia,” he said, with interests in military espionage, for example. But there have been “several” APT groups seen targeting Russian victims, he said.

Kurt Baumgartner, principal security researcher at Kaspersky Lab, says the increased activity targets “a geopolitical profile.”

Industries that support those geopolitical interests and structure are also under attack, he said.

CrowdStrike also has seen more Chinese attacks on Russia -- from a specific Chinese APT group called Hammer Panda against Russian Federation nations. But it's also still seeing China-based attacks on US companies.

"We have definitely observed an increase in Hammer Panda targeting of the Russian Federation. In the [CrowdStrike] Global Threat Report ... we observe that following an agreement between China and Russia in May 2015 to abolish any type of hacking between the two states, we observed an almost immediate violation of the agreement by China," said Adam Meyers, vice president of intelligence at CrowdStrike. "We have continued to observe China-based intrusion groups targeting US companies."

Find out more about APTs at Interop 2016, May 2-6, at the Mandalay Bay Convention Center, Las Vegas. Register today and receive an early bird discount of $200.

Vulnerabilities/ThreatsThreat IntelligenceAttacks/BreachesAdvanced Threats

Keep up with the latest cybersecurity threats, newly-discovered vulnerabilities, data breach information, and emerging trends. Delivered daily or weekly right to your email inbox.

Subscribe