China, Romania key sources of hacking, report says

April 23 2013

A person walks past a 12-story building alleged in a report on February 19, 2013 as the home of a Chinese military-led hacking group in Shanghai's northern suburb of Gaoqiao. China and Romania were by far the largest sources of confirmed hacking attempts last year, with China's mostly from state-controlled sources aimed at data theft, a new report said Tuesday.

China and Romania were by far the largest sources of confirmed hacking attempts last year, with China's mostly from state-controlled sources aimed at data theft, a new report said Tuesday.

Verizon's 2013 Data Breach Investigations report said 30 percent of 621 confirmed attacks were sourced back to China, 28 percent to Romania, and another 18 percent to the United States.

By far most of the attacks in China were focused on data theft, the report said, while those from Romania and most of those in the United States were about theft for financial gains.

"State-affiliated actors tied to China are the biggest mover in 2012. Their efforts to steal IP (intellectual property) comprise about one-fifth of all breaches in this dataset."

"This may mean that other threat groups perform their activities with greater stealth and subterfuge. But it could also mean that China is, in fact, the most active source of national and industrial espionage in the world today."

The report was compiled together with 19 groups from the global computer security and law enforcement community, many of them national cybersecurity organizations and public-private computer security groups.

The report said there were some 47,000 reported security incidents last year, the large part of them related to error, usually on the part of someone in a company who has lost a device or missent an email that could expose its systems.

But of those, there were 621 confirmed data breaches, three-quarters of them driven by financial motives.

Of the total, 111 were combined physical and malware attacks on smaller establishments aimed at financial theft.

Another 190 involved the physical penetration of bank automatic teller or cash point machines, using skimming devices to steal customer data.

And 120 more were what the Verizon report called the standard technique for penetrating networks and data for financial and espionage reasons: a mix of malware, hacking, phishing and other techniques.

Out of the 621 breaches, 19 percent came from state-linked actors, almost all of those from China, and were not financially driven, the report said.

Those from Romania, Russia and Bulgaria—40 percent of the total—were virtually all aimed at financial gains.

(c) 2013 AFP