Encore! APT17 hacked Chinese targets and offered the data for sale

intrusiontruth.wordpress.com/2019/07/25/encore-apt17-hacked-chinese-targets-and-offered-the-data-for-sale/

intrusiontruth July 25, 2019

We started this story with Guo Lin (郭林), identified to us as an MSS Officer. We showed that he had personal links to a number of companies and individuals involved in Cyber security, at least one of whom helped develop a key tool used by APT17. We have also shown direct links between Guo Lin's company Antorsoft and the Chinese Ministry of State Security.

But what were APT17 really doing? We know from media coverage in our part of the world that APT17 hacked a number of targets in the West and did untold damage. What isn't well known is that they were also hackers for hire, acquiring data and selling it for profit.

The sales brochure

The images below show a 'Price List' made available to this blog by an analyst working with us. Members of APT17 actively circulated this list amongst the hacking community in China seeking buyers.

The list shows data for sale, and not just from Western companies…

Either, APT17 has some sort of domestic remit, acquiring data on Chinese citizens and selling it to the MSS (but that is unlikely, because China's new intelligence law compels companies to provide information required by the government, and the price list certainly wouldn't be circulated online).

Or, the MSS has lost all control of APT17, which is hacking Chinese victims and selling the data to the highest bidder.

Which do you think?