Is there a pattern?

intrusiontruth.wordpress.com/2019/07/15/is-there-a-pattern

intrusiontruth July 15, 2019

Readers of this blog will know that our investigations into APT3 and APT10 started with well-known intrusions and ended with the identities of the perpetrators and the identification of a front company connected to the Chinese Ministry of State Security (MSS).

As we pointed out on Twitter in December, there seems to be a pattern developing – a regional office of the MSS creates a company, hires a team of hackers and attacks Western targets. Why the MSS insists on using sloppy contracted hackers is beyond us here at Intrusion Truth, but the pattern is undeniable.

What *isn't* clear is how widespread it is. As we asked in December, **what if *all* regional offices of the MSS have their own APT?** Could the trail of crumbs be followed in reverse?

Could we start an investigation with an MSS Cyber Officer and identify the APT they manage?

Starting with the MSS

We recently received a tip from a friendly source that prefers to remain anonymous, but whose identity we have independently verified. The source named an individual based in Jinan, a sprawling city famous for its many natural springs. The source claimed that the individual worked for the MSS on Cyber issues and might be involved in APT hacking.

This was the perfect opportunity to look for an APT and to test our hypothesis.

Experts working with this blog conducted an investigation.

We will bring you the results this week.

#weknowwherethisleads