KCS
Strategic Intelligence & Corporate Security

May 2022

Mustang Panda, Hidden Dragon

'Bronze President' is not just another nickname for Donald Trump. It is a Chinese state-sponsored hacking group that has historically operated in the South Asian region, working across Hong Kong, Vietnam, and Burma (Myanmar), to gather sensitive information of interest to Beijing in its own backyard. But there are signs that the group's targets are changing. Multiple reports from the past month indicate that the group, which is also known as Mustang Panda and Red Delta, is now pivoting to focus on gathering intelligence from Russia, in a reminder that no matter who your friends may be, those closest can better wield the knife.

China has hovered between neutral and Moscow-favouring in its response to the invasion of Ukraine, calling for a peaceful resolution but notably, not joining in any sanctions or official condemnation, and pledging to continue to work with Russia regardless of the outcome. This is broadly what was expected – with China and Russia forming an authoritarian bulwark at UN level since 1945 and forming close political and economic relationships, not least through the BRICS grouping. In truth, China's cyber-snooping on Russia is also to be expected – allies watch each other as closely as they watch their enemies. What is surprising is that it is one of China's top Advanced Persistent Threat collectives being redeployed, highlighting that China currently considers the Ukrainian conflict – through both directly targeting Russian systems, and European governments & NGOs related to the war – as a high priority.

As far as the attacks on Russia go, China rightly sees its partner as reeling from the ongoing (arguable) failure of the war and the sheer weight and scale of the sanctions, and assesses Moscow as being the weakest it has been since the collapse of the Soviet Union. Targeting military and government victims in Russia, therefore, could give China the 'edge' on understanding Russia's intentions and greater leverage in persuading Russia – which does not have many friends left, much less ones as powerful – to take a course that ultimately favours Beijing's interests. The specific targeting of Russian-language users supports this. Of course, there is also an element of the Chinese doing this just because they *can*, and that any opportunity to exploit an ally is fair game.

In terms of the targeting of European corporates and government/diplomatic entities, the aim goes beyond simple intelligence-gathering, and the Ukrainian conflict is used as the 'lure' rather than seen as the endgame. Diplomats awaiting official briefings, corporates keen to learn how their financial position will be impacted, and individuals just following the conflict out of grim interest, will all be likely to fall prey to email phishing exploits that look and sound the part, but which contain malware to load a Trojan, execute commands or even take remote control, in addition to the standard data theft.

This tactic of capitalising on a crisis was previously seen not too long ago in the coronavirus pandemic, with Covid-related cyber fraud pushing cybercrime 15 times over. With the Ukrainian war, it seems that the main threat actors – to date at least – are state-sponsored ones looking for information and control, rather than opportunistic financially-driven criminals. However, a successful strategy rarely remains in isolation for long and the Chinese cyber-espionage is envisioned to become just one of multiple strands by which the Russian invasion will raise the risk and threat profile for entities of any type, worldwide. As with last year's revelations about the NSO, there is a greater degree of professionalisation in, and acceptance of, cyber compromises and the impact of these cannot be understated. Particularly if, as China has proven with its targeting of Russia just as much as the West, no distinction is made between friends and enemies.

The cyber front was always going to be the most serious for the world in the new millennium, despite Russia's ongoing attempt to dare the rest of the planet into World War III. The political angle seen in Mustang Panda and Bronze President certainly adds a further degree of spice and severity. However, it is important to remember that for nations such as China and Russia, there is often little between what counts as a private venture, and a state one. Corporates have always been acceptable targets - it is just that now, with the war dominating political and economic discourse, the arrows fly truer than ever.