No-limits relationship? China’s state hackers scoop up intelligence on Ukraine… and Russia

intrusiontruth ⁝⁝ 12/24/2022

#2023lifegoals

As we near the end of 2022 we wanted to finish with our opinion related to the Chinese hacker paradise. Not the beaches on Hainan island, but the networks of Ukraine and Russia…

This is something we have taken an interest in since we Tweeted on 15 March 2022 so wanted to pull together some fantastic work that is out there for our community as a little ‘night cap’ before we get back to shining a light on the Chinese cyber machine, exposing their villainous activity and to enable them to ditch their state sponsored computer and escape to Hainan island in 2023.

So pull up a chair, grab a drink and snack of your choice and let’s dive in together.

Russian invasion of Ukraine

For a while we have been researching and reporting on Chinese state cyber activity around the globe. Their malcontent for the rules-based order is evident as is their disregard for intellectual property with all the hard work that goes into this.

24 February 2022 is a date that will forever be etched in the minds of the Ukrainian people and the world as the day the Russians decided to invade Ukraine. The images of the atrocities carried out in Bucha by the Russian army is just one example of the horror show being conducted by the Russian military. The world in unison condemned this activity, but the Chinese Community Party (CCP) was somewhat absent coming just weeks after President Vladimir Putin and President Xi Jinping declared their “no-limits” partnership. Which makes us question: Did the CCP know? Actions speak louder than words.

The Chinese state's reaction was initially one of neutrality before rolling back as the relationship became an embarrassment to China. Most evident of all was President Xi Jinping signing the final declaration at the G20 summit in Bali, condemning the Russian invasion of Ukraine. Was the partnership ever anything more than a ruse by the CCP?

Now, as we have all seen through the year, it's not going well. So is the public image of the "no-limits" relationship the full story?

"wait, you are going to invade where?"

Chinese state hackers get involved

In March 2022 the Ukrainian 'computer emergency response team (CERT-UA)' issued a warning about cyberattacks on the countries police agencies. The activity was via phishing emails with HeaderTip malware included inside weaponized documents. The message when translated stated "*on the preservation of video recordings of the criminal actions of the army of the Russian Federation.rar*" which also included an executable with the same name. All of this could easily point back to Russian state hackers. They are invading Ukraine and as such would want to know what is going on in the country. However, an investigation by SentinelOne identified the link between the HeaderTip malware and "scarab" which has links to the Chinese government. This is a fantastic bit of work by SentinelOne exposing a clear link to the Chinese state. This activity is reported within a couple of weeks of the Russian invasion of Ukraine, with Check Point Research (CPR) also flagging that the "frequency of cyberattacks from Chinese IP addresses around the world jumped 72% in the week from March 14 to March 20, compared with the seven-day period before the Russian invasion of Ukraine began". Why such an interest from Chinese state hackers in Ukraine? Our next stop is to what was happening before the Russian invasion.

On Friday April 1st, 2022, The Times UK released an exclusive outlining the Chinese state's hacking activity. According to this article, this activity had occurred during the Beijing winter Olympics up to 23 February 2022 (the day before the Russian invasion of Ukraine). What is interesting is that the source stated the hack was widespread, across "600 websites belonging to the Ukrainian defense ministry" but also "Ukrainian government, medical and education networks".

Chinese state relationship with Russia

So, are we seeing the “no-limits” relationship at work behind the scenes? Having reviewed other avenues there is a mixed picture. Where we see hacking in Ukraine by Chinese state hackers, we also see reporting of Chinese state hackers targeting Russia itself. Of note, SentinelOne state that the Chinese hacker group Scarab mentioned above has previously targeted Russia in a quest to hack, interpreting the “no-limits” relationship tagline in a different way to the Xi Jinping of early February 2022…

As outlined in the National Interest, the CCP is vying to become a “cyber superpower”. It has the numbers, not necessarily the talent, but is a highly capable thief (just ask all the companies who have lost intellectual property over the years). Is this just the Chinese state stealing all the data for themselves? As Tim Starks and AJ Vincens wrote in July 2022 “the Ukraine war could provide a cyberwarfare manual for Chinese generals eying Taiwan” but you could argue it is more than that. China is surpassing its Russian ‘comrade’ and will take advantage of any opportunity to acquire all the information it can get.

@remonwangxt

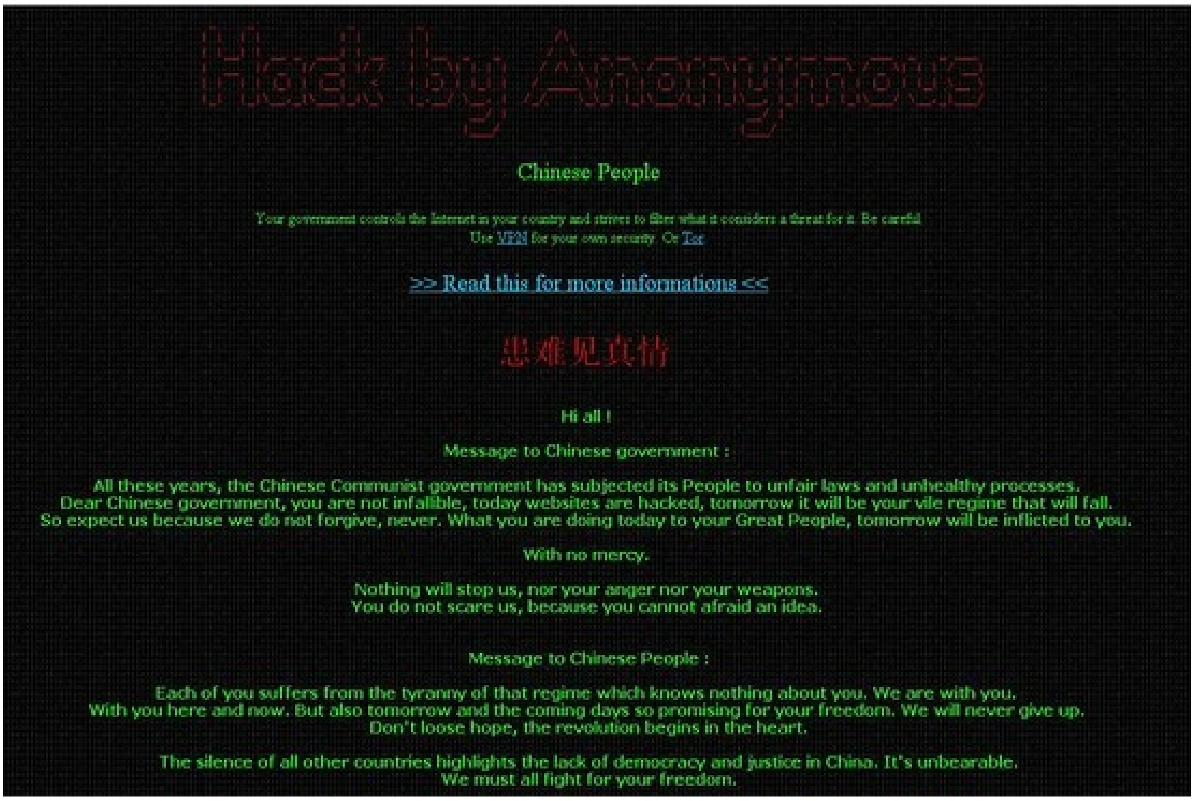
Not so much a relationship….

On this note, we move to the Chinese state’s targeting of Russia. We start with a piece by CPR in May 2022. Another phishing attempt, another set of emails, another Chinese state cyber hack but this time the target was Russian military research and development institutes (with Belarus thrown in for good measure). What is that saying, ‘all is fair in love and war’? Well, we have love between Xi and Putin, but when Putin’s eyes are on Ukraine, Xi is stabbing his comrade in the back. CPR also flagged that this targeting had overlaps with Stone Panda and Mustang Panda. This seems like a homerun to us.

In a friendship of equals some are more equal than others…and the Russians seemed to know the Chinese state are hacking them to their hearts content. Kaspersky identified Chinese state sponsored hacking activity as early as January 2022. Reported in August by Spiceworks, “Kaspersky blamed Chinese state sponsored hacking group TA428 for a number of phishing attacks targeting industrial plants, research institutes, government agencies and ministries across Russia, Belarus, Ukraine and Afghanistan”. The use of a 17-year-old memory corruption (CVE-2017-11882) was ‘in’ before utilising TTP’s distinct to TA428 with sensitive searches being conducted. Now I don’t know about you but does the above look like an ally you want in a “no-limits" relationship? What were these Chinese state hackers looking for? If you ask us, the Russians clearly are aware of the Chinese state's hacking campaign against them. They aren't exactly covering their tracks. The Russian government is desperate, along and weaker than ever.

Dragonbridge and fighting back

Yet all hope is not lost. We are aware we are swimming against the tide here; it appears the CCP is relentless and cannot be stopped. But during a Wikipedia edit war which the hacktivist collective Anonymous state is part of a Chinese influence operation to remove information from Wikipedia, Anonymous hacked the Chinese Ministry of Emergency Management among other websites. It highlights that China's 'Great Firewall' is prone to attacks and exploitation.



Hack by Anonymous

Chinese People

Your government controls the Internet in your country and strives to filter what it considers a threat for it. Be careful.
Use VPN for your own security. Or Tor

>> Read this for more informations <<

患难见真情

Hi all !

Message to Chinese government :

All these years, the Chinese Communist government has subjected its People to unfair laws and unhealthy processes.
Dear Chinese government, you are not infallible, today websites are hacked, tomorrow it will be your vile regime that will fall.
So expect us because we do not forgive, never. What you are doing today to your Great People, tomorrow will be inflicted to you.

With no mercy.

Nothing will stop us, nor your anger nor your weapons.
You do not scare us, because you cannot afraid an idea.

Message to Chinese People :

Each of you suffers from the tyranny of that regime which knows nothing about you. We are with you.
With you here and now. But also tomorrow and the coming days so promising for your freedom. We will never give up.
Don't loose hope, the revolution begins in the heart.

The silence of all other countries highlights the lack of democracy and justice in China. It's unbearable.
We must all fight for your freedom.

The message was on a number of Chinese sites, including on government sites

And on something we haven't commented on but wanted to wind up with. It would be rude not to mention the botnet menace from Dragonbridge. First flagged by Mandiant in September 2021, not only are the Chinese state hackers stealing intellectual property but they are shifting to the influence game. We see Dragonbridge target events in the US and clearly, we are hitting them where it hurts as they turned their attention to us recently in an attempt to shadowban our content. Now – don't get us wrong. It is nice to be noticed by the Chinese state hackers. I means we are getting under their skin. But it's a global redline when they are targeting the Ukrainians with disinformation. Now Dragonbridge hasn't really been that effective. In our case, having the community identify and flag these accounts has ensured it didn't really make much of a splash. Thank you to everyone who contributed to spotting Brandi, Monique and the rest of the botnet bandits!

Now both examples demonstrate that although the CCP want to be seen as a "cyber superpower"; they really aren't. As a community we can continue to expose Chinese state hacking activity, the actors behind the keys and the hypocrisy of the Chinese state. All it takes is that continued vision from the community to flag this hostile activity, keep running down those leads and continue to help us in our quest for the truth.

And finally…..

So alas, the Chinese state hackers are not sunning themselves on a beach, enjoying some time away from the keys and considering a more productive and fulfilling life away from their CCP puppet masters. Instead, they continue to look for any opportunity to target people, companies or countries. Even when those countries are simply fighting for their independent survival….

We hope that these Chinese state hackers walk away from their keyboards in 2023. However, our New Year’s prediction is that they will continue and as such this community needs to stay the course in exposing malign cyber activity: for our loved ones, for our brothers and sisters in Ukraine and for the hard-working people across the globe whom the CCP steal and hack at will.

As always, you know how to get in touch.

Wherever you may be, we wish all our readers a happy holiday. We will be back in 2023. See you for the fireworks.