APT41: A Case Sudy

intrusiontruth ⋮⋮ 7/20/2022

As you know, we have been dedicated for some time now to revealing the truth behind state-sponsored, managed or directed intrusion sets. We have learnt more about the way in which the Chinese state conduct their criminal cyber activity and how it has evolved over the years.

Chinese APT groups are aggressive, persistent, and garner a large network of criminal hackers. The Chinese state uses this model to promote their agenda and provide protection to the common cybercriminal. This model is fallible which allows us to promote the truth behind these intrusion sets.

Nevertheless, the CCP continue to outwardly lie to protect their international and domestic reputation. They do this whilst simultaneously supporting cybercrime and allowing huge networks to profit from its illegal activities. The Chinese state is asserting do what I say, not what I do.

APT41: What we know

APT41 is a difficult group to pin down/classify/group. It is a group with many names: WICKED PANDA/DOUBLE DRAGON/WICKED SPIDER/WINNTI GROUP, the list appears to go on.

Early intrusions by APT41 traditionally focussed on the international gaming sector, reusing stolen code-signing certificates for malware distribution. Indicted APT41 actors registered gaming domains which later went on to serve as a means to fraudulently obtain gaming currency (through the Malaysian company SEA Gamer) and establish backdoors into international gaming companies to facilitate the spread of Chinese intrusions.

Their focus on the gaming industry became a tangible lead against the group, with a heavy focus in countries such as Malaysia, Indonesia and Thailand. Timing as always is crucial. This early APT41 activity focused on the gaming industry at a time when the Chinese state was mandating growth in the gaming sector.

Over the past few years, APT41 has evolved. No longer is the focus purely on the gaming industry. Rather we have seen evidence of APT41 creating front companies in the computer and technology sector, claiming to employ pen testers and software developers which all supports the MSS model we have come to know well. It serves their aim of continuing to use highly aggressive techniques to support China's ambitious development targets alongside State Security Departments.

As FireEye neatly evidence, APT41 juggle their commitments to the Chinese state in the day (using the 9-9-6 model [9am-9pm, 6 days a week]) whilst hacking for financial gain in the evening. In some cases,

using state-level malware across both activity streams.

APT41 stands out due to its prolific use of non-public malware outside of working hours. They also share this malware with other cyber hackers in China, who work to various regional State Security Departments.

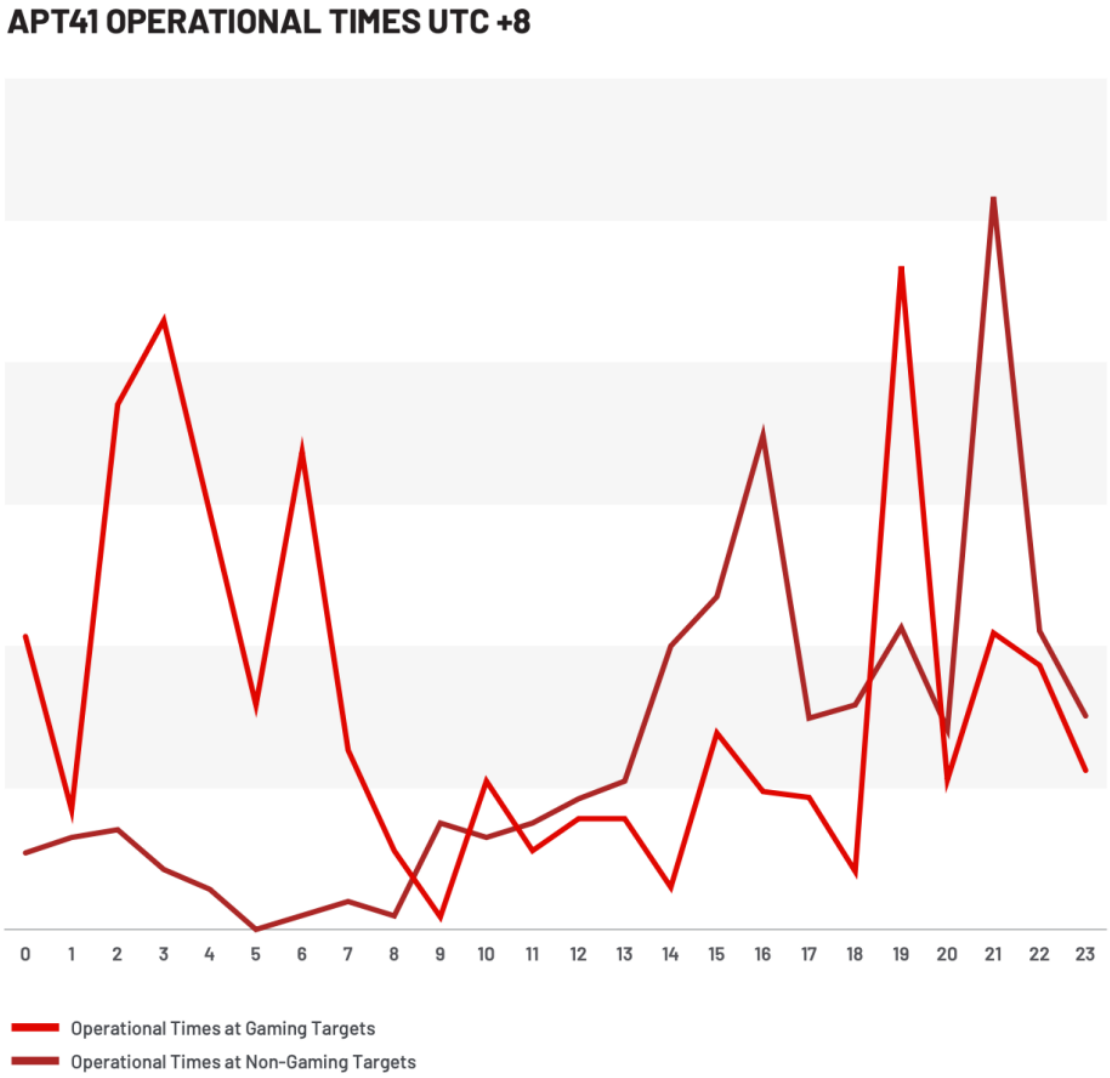

FIGURE 4. Operational activity for gaming versus non-gaming-related targeting based on observed operations since 2012.

China's state priorities and subsequent APT41 victims

The culmination of APT41's targets point to clear tasking from the Chinese state rather than a criminal entity. It serves to highlight the state's backing of groups such as APT41 and the degree of coordination behind the scenes.

For example, APT41's exfiltration of intelligence from vaccine development and healthcare institutes in order to advance the CCP's knowledge and gain an illegal, competitive edge. APT41 have taken advantage of the Coronavirus pandemic by hacking COVID-19 research and stealing IP in order to fast-track the Chinese-state's somewhat questionable vaccine supply.

Some readers will have noted APT41's vast victims in the indictment. One of interest to us was NGO16: A non-profit organisation dedicated to alleviating worldwide poverty. APT41 compromised this organisation and put the livelihood of fellow humans at risk. It is increasingly clear the morals of the criminals behind this group are non-existent.

Chinese APTs don't simply target international companies. They also target their own citizens using malware from big data capture to allow direct oversight of text message logs of high-profile Chinese targets. APT41 have systematically targeted hotels prior to senior officials staying in order to retrieve personal and identifiable information. This sort of direct, timely and specific targeting adds to the body of evidence that the Chinese state outsource at least part of their intrusive surveillance program to criminals within its borders.

It appears US indictments are not having the same effect as they used to. Back in February, Mandiant reported on APT41 re-comprising US government victims, and using niche animal healthcare apps such as USAHERDS to gain access to intelligence to serve the CCP data machine.

Despite five of the actors being doxed by the US in 2020, APT41 TTPs have continued to be pop up on our radar. Their interest recently? Universities.

Recent Targeting

And not just any universities. Universities in locations the CCP are concerned about: Taiwan and Hong Kong.

As already noted in the OSINT community, RouterGod is a known, custom malware tool used by Wicked Panda (APT41). We have observed sustained connections to RouterGod command-and-control servers from multiple IP addresses associated with Hong Kong universities, including the Hong Kong University of Science and Technology and Education Universities

As recently as March 2022, APT41 were using a VPS at Romania-registered IP address 91.238.50.114 to host "watson.misecure.com". We have seen evidence that they used this domain to compromise National Taiwan University databases using the "xp_cmdshell" (T1059.003) tool (to execute commands for netstat, process list, and network configuration) and successfully exfiltrated personally identifiable data on staff, students, and alumni of the university.

It appears nothing is off limits to this group. Any and all data is up for grabs.

Summary

We know the CCP uses criminal hackers to do their dirty work. Due to their lack of skill at evading detection, we also have the names of five individuals linked to Chinese intrusion set APT41.

The contractor model is no longer a neatly packaged, self-contained concept. The continuation of APTs engaging in dual hatting despite this now being public knowledge speaks to the Chinese state turning a blind eye. Repeated for-profit hacking makes it highly unlikely that APT41 is operating without the state's awareness. And despite being named and shamed in public indictments, this still does not deter the group's continued hacking of CCP's targets – most recently we have reported on this occurring in the

Education sector, with students, staff and alumni falling victim and their sensitive data stolen to feed the CCP data machine.

APT groups appeal because they are aggressive, dispensable and ‘distanced’ from the state-run organisations that sit behind them. We will continue to shed light on these cracks within the system; it is only a matter of time before this model becomes untenable. There is a lot of good work going on in this field (e.g, the Hearing on China’s Cyber Capabilities in the US) but we need to do more and keep applying the pressure. This is not just a US problem.

The rest of this series will look into who the APT41 indicted actors are. How are they connected and how does this fit into the complex web that is APT41? Stay tuned…