KCS Group Europe

Hacking in Brazil: Order and progress?

16/08/2018

Plot the key jurisdictions where hackers find the warmest welcome and you would likely come up with the usual suspects: Russia, China, Israel and so on. But one name sits a little incongruously on the list: Brazil. How is it that this state with no state-sponsored *'hacker armies'*, and not a major player in the political conflicts from which these stem, is one of the most cyber-crime afflicted states in the world, and what impact is this having on the state of affairs in the rest of the country?

Brazil may be newer to the hacker game than the above countries, but there are several factors that make it a major haunt of the cyber populace. For a start, its sheer size: with a population of over 200 million, with over 50% having regular online access, mean that this is a pool with fish of all sizes to be hooked. Second, its early adoption of online and automated finance over the past thirty years which provides the opportunity and methodology. And not to be forgotten, Brazil's role as the leading economic power of South America and of the BRIC movement as a whole.

However, these things by themselves are not enough: they must be matched by a permissive legal/bureaucratic culture, and the inability/unwillingness of the empowered to pull free of the corruption. In both of these instances, Brazil is once again open season for cybercrime. With no data protection authority, severe weaknesses in outward protection of websites (as evidenced by the takedown of five key Olympic-related websites on the eve of the 2016 Games) and a battle between the 'security' and 'privacy' factions over the future of the Internet – not to mention ineffectual and watered-down laws and penalties, and Brazil becomes more appetizing by the minute.

So, what are the precise dangers and threats? For such a strong financial market, as can be expected a lot circles around banking and financial transfers. Sometimes this is standard breaching of accounts or electronic fraud through diverting genuine payments to non-genuine accounts. But Brazil also has a particular payment system called the *boleto* – a bar code printed on paper that, when scanned, makes a transfer, and which was intended to remove the need to do so much online. *Boletos* can now be rewritten by cyber-criminals. Moreover, Brazil is a world leader in the production and dissemination of Trojans, not only those directly targeted against financial institutions but against the customers and general populace as well.

For the proof of the damage done, we might consider the attack that diverted every single customer of a particular Brazilian bank to rogue sites and which phished them for up to six hours. The cloning of stolen cards belonging to tourists at the World Cup and Olympics of this decade. Brazil's place as the number-one country, worldwide, for data breaches involving more than 10,000 records.

KCS Group Europe

Hacking in Brazil: Order and progress?

Moreover, the state of peace and security in the country is such that the police are not trained to, and do not have time to, deal with cyber-attacks when there is so much real-world crime going on. This has emboldened the Brazilian gangs to the extent where they openly advertise their services on social media (not even concealing themselves on the dark web) and promote physical 'schools' where one can go and learn the tricks – for a fee, of course. And in many cases, these new waves are not relying on the tools learned from Russia or China. They are creating their own.

A Kaspersky report into Brazilian cyber-crime had a damning indictment of the response: *'the law is not very effective… penalties are too lenient, and the judicial system is very slow'.* The chances of getting a swift and favourable outcome are minor so any attempt must be stopped before it has a chance to flourish. Systems should be genuine and up to date (any machine which uses a pirated version of Windows, as many do, is at extreme risk). Extreme skepticism should be taken with any requested transaction and, of course, full due diligence carried out on any potential partner to ensure that their cyber infrastructure and policies are just as robust as they should be.

Cybercrime laws were ultimately first passed in 2012 not because of a major corporate hack or loss, but because a Brazilian celebrity had intimate pictures stolen and posted online. This is emblematic of the problem: those in power did not act until a scandal hit the papers, rather than taking into account the already-latent problem infecting the corporate sector. Until the level of government response matches the efforts of the hackers, it is up to the individual companies to take the lion's share of the responsibility