Matt Sellman

SOCIAL MEDIA, CROWDSOURCING AND CITIZEN SENSING

How the Russian and Chinese governments are encouraging cyber-attacks against the United States and European countries and the impact of this on western assets.

What kind of crime are we dealing with?

The kind of crime that will be talked about in this essay will be the stealing of confidential information and disruption of infrastructure as an attempt to sabotage.

Firstly, an example of the differing attitudes between the east and west over hacking can be seen by an analysis of Google and Baidu results (Baidu being the censored Chinese version of Google). A simple search of Baidu looking for Chinese hacking returns a handful of primarily western news articles, most of which talk about the hacks taking place outside of China (KARPAL, 2015), CNBC being the most open. (A search for that articles URL in google finds returns a 404 error). Whereas a search of google for Chinese hacking ends up with hundreds of results from various sources, these include news outlets and Wikipedia among others.

Attacks made by hackers vary, there are direct attacks on infrastructure, intellectual property and social details such as customer databases (GRIMES, 2016). On the other hand, we have the Russian attacks, these appear to have been more focused on direct financial crime and social disruption. This is especially evident in the recent attacks on the elections in the USA and it is possible that the Brexit vote was also manipulated, although the latter has been unconfirmed (CRAIG, 2016), although I am inclined to agree. Currently, France and Germany, whose elections are due to come soon, are both bracing for possible attacks and interference by foreign nations.

Russia has proven itself to be as rich a source of hackers and hacking innovations as China, even outpacing the larger Chinese population in some respects, but failing in others, (THIELMAN, 2016). There is also the subject of the 'troll farms' used to spread disinformation within both the Russian and global community. This has been the case ever since activists started to use social media to protest the Kremlin, and ever since internet culture had begun to 'freewheel' without government interference. The troll farms have been used, not to spread pro-Kremlin interference, but rather to seed doubt and paranoia and to stop the internet being used as a democratic space (CHEN, 2016).

However, the more interesting point is the Russian interference in the US election. It is here where there has been a real break out into the mainstream media, and where there has been the most attention. Particularly interesting has been the unclassified intelligence report made by the CIA, FBI and the NSA. A particularly interesting line was: *"When it appeared to Moscow that Secretary Clinton was likely to win the election, the Russian influence campaign began to focus more on undermining her future presidency."* This shows us how unafraid the Russians feel when it comes to intervening in other countries and companies and how easily they can meddle with the affairs of another country without that much concern. Another interesting point is how this has been the report judges that this will *"We assess Moscow will apply lessons learned from its campaign aimed at the US presidential election to future influence*

efforts in the United States and worldwide, including against US allies and their election processes." (NSA, 2017). As I mentioned earlier, Germany and France are bracing against attacks by Russians and other countries to preserve the integrity of their elections.

But what are we, the west, doing? From the outside, it appears as if we merely accept these attacks and are instead focusing our attention on watching our own citizens. This can be seen in the IP bill in Britain (KILCOK, 2017). Something else that I have found rather interesting is that until the Snowden revelations (SNOWDEN 2013/14). There had been no idea of the scale of hacking made by the USA, both on its own citizens and on other countries. There is also evidence that the NSA has broken the cryptography in the HTTPS protocol (HALDERMAN, 2015). What this means is that the western secret services are either doing nothing towards Russia or China, or they are a lot subtler in their approach. Finding out which is made more difficult by how secretive Russia and China are when it comes to their flaws.

But how are these attacks made from China and Russia taking place? This is more technical: These attacks tend to be made using phishing, insiders and ransomware. Phishing is when an email, posing as legitimate, is sent to a user to gain access to personal information. This can also be called spear-phishing, when targeting a specific individual, or whaling, when targeting a specific CTO or CEO of a company. Insiders, as the name suggests, is where someone inside the company is either blackmailed, bribed or encouraged to let attackers access infrastructure such as databases or hardware inside the company, or by opening a 'backdoor', high level access without going through the company's main software, into the company, letting the attackers come and go as they please. Ransomware is when a piece of vital software, such as a database, is encrypted (usually using AES, since that is fastest) and the attackers only promise to decrypt it or give the user the private key when they hand over a certain amount of money. If the money is not given by a specific date, then the software is deleted. Sometimes the software is deleted anyway, even after the money has been given ().

These attacks appear to be mainly made by groups such as DeepPanda, FancyBear and CleverKitten – these names meaning country of origin, for example:

Nation-State and Non-Nation Based Adversaries

Panda = China
Bear = Russia
Kitten = Iran

India = Tiger
North Korea = Chollima (a mythical winged horse)

Jackal = Activist groups
Spider = Criminal groups

(MEYERS, 2014).

Where and why are these kinds of attacks happening?

The locations of these attacks vary, but the targets are normally the same. Usually the targets are companies and civilians. The Russians use these attacks are used to create confusion amongst the civilian population, sow distrust against anti-Russian targets and to promote Kremlin policies. Whereas the Chinese hackers are more focused on preserving their dominance against western targets, this tends to include attacking businesses and stealing intellectual property. These attacks are made to cause disruption, confusion and misinformation inside industry and civilian populations. The reason these attacks are occurring is simply because it is profitable. China has stolen millions of pounds' worth of intellectual property and Russia has destroyed confidence in the US presidential election. There is also evidence of attacks taking place on the oil and gas industry to preserve Russia's dominance in that area. (GRIMES, 2016).

Is it just eastern governments that are doing this?

Having looked at eastern European news sources I can say that there is no open evidence of attacks being made against either China or Russia. However, the truthfulness of these is doubtful given the nature of the censoring that goes on in both Russia. However, what there is evidence of is evidence of the civilian population of China being hacked. This is in part due to the restriction of hardware in China, *"The government's efforts to control the internet make domestic users more vulnerable, says FireEye's Boland. Beijing recently stepped up enforcement of a prohibition on the sale or import of hardware and mobile devices containing Trusted Platform Module microchips, used for encrypting passwords and biometric data"* (KREBS, 2015). What this means is that the international standard of cryptography, which protects western businesses, is non-existent in China, leading to companies having to use untrusted, older hardware and software that does not have security patches installed and therefore cannot be protected from malicious attacks by hackers who have the latest exploits from online.

But, in China, where the internet is censored, how do these hackers get these exploits? In China, there is 'Great firewall of China', a blacklist of internet addresses that is deemed dangerous or objectionable by the government (AUGUST, 2007). However, this firewall can be bypassed by the terracotta VPN, this is a VPN with over 1500 nodes around the world. These nodes tend to be servers and computers that are laughably vulnerable, some having no security whatsoever (KOROLOV, 2015).

Chinses hackers use this to break out into the wider world and access information available in the wider world. What this means is that they can easily use the latest security flaws on the outdated Chinese systems. It is not only the fact that they can 'escape' the Chinese blockade, there are Chinese employed hackers who work outside of China to hack western targets (KARPAL, 2015). Another thing that makes the VPN notable, is that it originates in China and is notably used by the hacking group DeepPanda (BEARDMORE, 2015).

On the other hand, I could not find any evidence of Russians being hacked or attacked, but what I did find was evidence of the poverty of the Russian people being exploited by the Russian government and the Russian mafia, both working hand in hand with one another. These organisations appear to take advantage of bored and unemployed teenagers who break and crack things to make a living and use them against the west in sophisticated attacks. (RCUBED, 2016). This is shown in the recent attacks on Ukraine's power grid, which caused it to shut down for some time (OLIVIA, 2017).

Thoughts on the future:

Current trends predict that there will be a greater number of attacks focused on smartphones, alongside an increase in ransomware and the internet of things being used to create DDOS attacks. (S-CONNECT, 2017). This will be done alongside an increase in Russian interference in both the social and physical life of western civilians. The Chinese population will, until their government allows the latest cyber security hardware into the country, continue to be hacked and exploited, with or without their knowledge. The UK will continue to watch its citizens and perhaps monitor the efforts of other countries. The US will have the Donald in charge, so it is unclear as to what they will be doing.

Bibliography

Assange, J., 2006 onwards. *Wikileaks.* [Online]
Available at: Wikileaks.org
[Accessed 11th January 2017].

Beadmore, P., 2015. *Terracotta VPN: Enabler of advanced threat anonymity.* [Online]
Available at: https://blogs.rsa.com/terracotta-vpn-enabler-of-advanced-threat-anonymity/
[Accessed 15th January 2017].

Chen, A., 2016. *The real paranoia-inducing purpose of russian hacks.* [Online]
Available at: http://www.newyorker.com/news/news-desk/the-real-paranoia-inducing-purpose-of-russian-hacks
[Accessed 10th January 2017].

Craig, J., 2016. *Russian hackers 'probably swayed Brexit vote', says Ben Bradshaw MP.* [Online]
Available at: http://news.sky.com/story/russian-hackers-probably-swayed-brexit-vote-says-ben-bradshaw-mp-10694779
[Accessed 17th January 2017].

Grimes, R. A., 2016. *InfoWorld.* [Online]
Available at: http://www.infoworld.com/article/3132068/security/which-country-has-the-best-hackers-russia-or-china.html
[Accessed 3rd January 2017].

Halderman, A., 2015. *Freedom to Tinker.* [Online]
Available at: https://freedom-to-tinker.com/2015/10/14/how-is-nsa-breaking-so-much-crypto/
[Accessed 12th January 2017].

Karpal, A., 2015. *China hacking US companies for secrets despite cyber-pact.* [Online]
Available at: http://www.cnbc.com/2015/10/19/china-hacking-us-companies-for-secrets-despite-cyber-pact-.html
[Accessed 4th January 2017].

Kilock, J., 2017. *The IP Act: UK's most extreme surveillance law.* [Online]
Available at: http://www.aljazeera.com/indepth/opinion/2016/12/ip-act-uk-extreme-surveillance-law-161201141317587.html
[Accessed 14th January 2017].

Korolov, M., 2015. *The Terracotta commerical VPN.* [Online]
Available at: http://www.csoonline.com/article/2956433/advanced-persistent-threats/terracotta-vpn-hijacks-servers-for-commercial-gain.html
[Accessed 15th January 2017].

Krebs, B., 2015. *KrebsonSecurity.* [Online]
Available at: https://krebsonsecurity.com/2015/08/chinese-vpn-service-as-attack-platform/#more-31771
[Accessed 15th January 2017].

Meyers, A., 2014. *Meet the Adversaries.* [Online]
Available at: https://www.crowdstrike.com/blog/meet-the-adversaries/
[Accessed 16th January 2017].

NSA, F. a. C., 2017. *Intelligence Report on Russian Hacking.* [Online]
Available at: http://www.nytimes.com/interactive/2017/01/06/us/politics/document-russia-hacking-report-intelligence-agencies.html?_r=1
[Accessed 10th January 2017].

Olivia, 2017. *UNM4SK3D: Ukraine, Altaba, and St. Jude.* [Online]
Available at: https://www.cybrary.it/2017/01/unm4sk3d-ukraine-altaba-st-jude/
[Accessed 14th January 2017].

Rcubed, 2016. *Why are Russians Such Talented and Determined Hackers?.* [Online]
Available at: https://www.cybrary.it/2016/12/russians-talented-determined-hackers/
[Accessed 15th January 2017].

S-Connect, 2017. *2017 Cyber Security Trends.* [Online]
Available at: https://www.cybrary.it/0p3n/cyber-security-trends-2017/
[Accessed 13th January 2017].

Snowden, E., 2013/2014. *Snowden Revelations.* [Online]
Available at: https://www.lawfareblog.com/snowden-revelations
[Accessed 6th January 2017].

Thielman, S., 2016. *DNC email leak: Russian Hackers Cozy Bear and Fancy Bear behind breach.* [Online]
Available at: https://www.theguardian.com/technology/2016/jul/26/dnc-email-leak-russian-hack-guccifer-2
[Accessed 2rd January 2017].