Cyber Warfare: An Era of Nation-State Actors and Global Corporate Espionage

By Joab Kose – Incident Response & Security Researcher

The last decade witnessed the highest rise in state-sponsored Cybercriminal activities, with the most recent Russian-linked SolarWinds breach that impacted most of the US governmental and non-governmental organizations, confirming how dangerous these threats can be.

Executive Summary

The last decade witnessed the highest rise in state-sponsored Cybercriminal activities, with the most recent Russian-linked SolarWinds breach that impacted most of the US governmental and non-governmental organizations, confirming how dangerous these threats can be. These types of attacks are performed by Advanced Persistent Threats (APT) groups, with specific missions on their target victims. APTs are hacking groups that are sponsored and funded by governments. The groups are well-organized, highly skilled, experienced, and determined. They have strategic modes of operations. It is publicly known that countries like Russia, China, Iran, , the USA, Israel, and North Korea, own hacking groups that are trained and well-resourced to carry out specific missions in the interest of their countries. This article takes an in-depth look at the cyber threats from the state-sponsored cybercriminal groups and cyber-espionage activities they are involved in. I must state that this article reflects my own opinion, based on studies, research, and other articles that have been published, and not the publisher or the association's opinion.

Keywords

Advanced Persistent Threats (APT), Cyber-Espionage, State-Sponsored Attack, China, Russia, Iran, North-Korea.

Introduction

In 2019, the world was shocked by the revelation about the C919 airplane which was manufactured by a Chinese state-owned aerospace company known as Comac. It turned out that the airplane was a product of a Chinese global hacking operation leading to the illegal acquisition of intellectual properties (IPs) of different parts of the plane, from several foreign companies like Ametek, Honeywell, Safran, Capstone Turbine, and GE, among others, between the year 2010 and 2015. It is reported that this was a multi-year well-coordinated hacking-campaign sponsored by the Chinese Government, in its attempt to bridge the technological-gap in China's aviation industry. [7] While this alone might sound scarey, China is not the only threat actor in this kind of operation. Russia, Iran, and North Korea have proven their nation-states' cyber-capabilities through offensive operations like discovering secrets, stealing corporate data (intellectual property), corrupting individuals through political disinformation, spying on specific targets, disrupting operations, and destroying critical infrastructures of other nations. [6] However, China has been the main player in cyber-espionage, which is the focus of this article.

With the realization of the opportunities that cyberspace is offering, governments across the world are building on Cyber-forces, which are tasked with accomplishing their specific goals and agendas against other states. [4] Nation-state actors are well-trained, resourced, and equipped to disrupt, steal, and interfere with other nations' economies, governance, and military capabilities. APTs differ from other criminal hackers in several ways: they are normally not interested in personal gain, and they engage in long-term cyber operations that could go undetected for several months or years. Protecting from APTs is challenging because their attacks are directed at several security layers of their victims, and they are super stealthy in their modes of operation. They deploy some of the most sophisticated techniques, tactics, and procedures that can go undetected by the security layers in place.

What is motivating Nation-state actors?

There has been an ongoing struggle for superiority, dominance, and relevance among the developed and developing countries globally. Superiority and influence are determined by certain aspects, like military strength, economic success, and the resources that a country possesses. For years, there have been restrictions, borderlines, and boundaries to dictate what one country could do to another. However, the advancement in technology has broken these barriers, and Cyberspace has offered the opportunity to those with the capability and willingness to utilize and take advantage.

To gain economic and technological power, some countries have resorted to climbing their way up the economic ladder through illegal means and shortcuts. This involves stealing the cutting-edge technologies and innovations from other countries that have invested a lot of their resources and time in research. There are key fields of interest like healthcare, aviation, military technology, among other sectors, in which a lot of intellectual properties are being stolen. China remains a bigger player in corporate espionage, and it uses all means, including cyber-intrusions and corrupting corporate insiders to gain access. [11] This is in addition to the disinformation and other cyber-criminal campaigns being carried out against other countries. The drive behind economic espionage to gain economic power and cyberspace is providing the platform for all these to happen.

According to Cimpanu, [7] China invests a lot of resources in the illegal acquisition of intellectual properties from different companies and institutions across the globe to achieve its economic and technological goals. The Chinese nation-state actors carry out their coordinated hacking campaigns, and sometimes when they hit the dead-end and unable to accomplish their missions through cyber-intrusion; they switch to corrupting some of the trusted insiders from their target companies. This has also been witnessed in the higher education and research institutions where some countries corrupt trusted researchers and graduate students to carry out their corporate espionage missions. [11] China is accused of sending its students and researchers as visiting scholars, to International research institutions, and using them to spy and steal research work across the globe. [3] According to the China Defense Universities Tracker, [5] China has a list of universities that are linked and integrated into the Chinese Military apparatus, intelligence community, and security agencies across China. Sending students and researchers from these institutions to foreign countries as visiting scholars creates the bridge for the wider espionage campaign.

How dangerous can the threats from Nation-State actors be?

In 2007, Estonia was hit by one of the deadliest and politically motivated cyber-attacks in history, and experienced an internet blackout for several days, exposing the capability and threats of state-sponsored cyber-forces. It later came clear that the attack was a result of the political conflict between Estonia and Russia, and it is believed that Russia was responsible for the attack. Estonia, being a small country with most of its activities digitized and connected to the internet, the DDoS attack disrupted critical operations like banking, transportation, and communication systems for days. [9] Three years down the line, Iran became the victim, with a deadly malware attack: Stuxnet, which was targeted at its Nuclear facility (Natanz uranium enrichment plant). This was a well-researched and perfectly executed attack that targeted a specific component used for controlling the centrifuges. Stuxnet became the first digitized weapon used against another nation, with the impact of bringing down the entire nuclear plant. [10] According to Rosenbaum, [13] the US and Israel possibly played a role in the Iran Stuxnet attack. In retaliation to Iran shooting down the US drone in 2019, it's believed that the US responded with a cyberattack that disabled Iran's computer systems used to control missiles and rockets' launchers. [14]

Nation-state actors pose a huge threat to their targeted victims because these APT groups deploy techniques, tactics, and procedures that have the potential of causing damaging impacts. This became very clear in 2014 when SONY got hacked by the North Korean state-sponsored hackers following the release of the movie "The Interview," in which North Korea claimed made fun of their president. Again, this was a well-executed attack that showed how governments have invested in their cyber-forces and capabilities to carry out specific missions. These instances show the impact and threats being posed by state-sponsored cyber-forces, and how far they are sometimes willing to go.

Targeted areas of interest by Nation-State actors

Nation-state actors have specific goals and areas of interest in their operations, and they invest heavily to succeed. Some of their missions are long-term and require more resources and skills to achieve. Others are short-term and instant, but still, need investment and sponsorship from their states. Each nation-state actor has a different interest and motivation, and research has shown that the major interests in foreign countries are intellectual properties (IPs), Political and governance interference, and military technology.

Intellectual Properties (IPs)

There has been a mass campaign for economic espionage from different countries, targeting specific sectors in selected countries. Many Chinese nationals were charged by the United States Department of Justice in 2014, in connection with corporate espionage against the United States corporations. Most of the charged victims were Chinese state officials working in different units from the PLA (Chinese People's Liberation Army). [2] China is well known to have perfected its art of espionage and has several APT groups tasked with stealing intellectual properties across the globe. Their main interest is cutting edge innovations in healthcare, technology, aviation, and transportation. The targets are mainly big companies across the globe that work on research and new cutting-edge technology products relating to satellite-industries, aerospace, and communication-industries. Russia is known to have built some of the powerful tools for cyber espionage. These tools include Mini-Duke, Cosmic-Duke, Onion-Duke, and Cozy-Duke, and are believed to have been built and used for cyber-espionage by a Russian Hacking group known as the DUKE. [4]

Political and Governance Interference

Foreign countries are becoming more interested in the decision-making process of other countries that have influence. This is a wider global cyber-campaign, mainly being led by Russia. [1] Through online disinformation, cyber intrusion, and corrupted insiders, the state-sponsored hacking groups are trying to interfere with politics and governance in other countries to gain global political mileage. The last decade recorded the highest political influence through online campaigns, and the revelation about Cambridge Analytica was just the tip of the iceberg of how decision making can be influenced through electoral processes. The Estonia hack, allegedly by Russia [9] in 2007 showed how political interests and conflicts can be a major precursor to massive cyberattacks, leading to losses and destruction of assets.

Military capability

A Chinese APT group by the name PUTTER PANDA has shown a lot of determination in conducting reconnaissance and intelligence gathering missions, with the United States as their target. According to CrowdStrike, [2] this group is targeting the United States Defense, Research institutions, and the technology sectors. The Defense contractors have been the main target for cyber-espionage, with British defense contractor QinetiQ having been compromised by an APT group linked to China. During this breach, the attackers were able to gain access to information about the United States' cutting-edge military drones and robotic-weapon systems. [8]

Attack techniques used by Nation-state threat actors

State-sponsored cyber-attacks are performed with greater precision. A lot of effort, research, and resources are invested before the real attack. Some of the techniques and methods used by the attackers include:

Cyber-Intrusion

Cyber intrusion is the main method used for stealing corporate intellectual properties and assets. This involves compromising the target systems and networks to gain remote access to obtain the data they need. The hacking groups have smart, skilled, and experienced personnel, with sophisticated tools that they used to compromise their targets. In most cases, they look for zero-day vulnerabilities to exploit.

Corrupting Trusted Insiders

On several occasions, the APT groups perform massive campaigns to corrupt the trusted insiders, to gain access to the organizations' information. Research has shown that most of the breaches are linked to the people who work with the companies and organizations being targeted. This type of attack is hard to detect and protect from because the people being used by the adversaries have approved access to the targets. During the Chinese global hacking operation between 2010 and 2015, that led to the acquisition of intellectual properties from different companies across the globe to build the C919 airplane, it is reported that when they could not obtain what they wanted through cyber intrusion, they could turn to bribe the people who worked in these companies [7].

Using graduate students and researchers

This is another method being used by foreign countries to steal research materials from research institutions. Research Institutions have become the focus and easy targets that admit foreign students and researchers under programs such as visiting scholars. The FBI charged Harvard's Chemistry department chairperson for having given false information that related to the Chinese talent-plan, and the PLA-Officer who was admitted at Boston University. It turned out that the PLA officer posed as a student while spying. FBI also reported that they arrested a Chinese-researcher who was stealing and smuggling biological-research vials in Boston. [11]

Disinformation through social media platforms

With the increased usage of social media platforms, the internet offers a cheaper and faster way of reaching large masses of people. Disinformation is another method used by foreign actors in their attempt to achieve their ill-intentions. The revelation about the Cambridge Analytica campaign to change peoples' views and decisions through the provision of misleading information, proved just how online-based disinformation could be used to change the course of countries' ways of life and reasoning.

Challenges from Nation-state attacks, and the way forward

Based on the trends that have been witnessed with the nation-state operations in the past years, it remains a challenge to protect organizations from state-sponsored Cyber-attacks and corporate espionage. Most of the known attacks have been noticed and detected after the breaches and damage. APTs deploy some of the most sophisticated methods in their hacking operations, making it harder and more difficult to be detected during the initial stages of the attacks, and even after gaining access. The biggest challenge is that these attacks always target different security layers of the organizations, including the exploitation and corrupting the trusted insiders with privileged access. This technique has been on the rise, especially with the corporate espionage campaigns from the nation-state threat actors targeting research institutions in other countries. A successfully executed attack from the Nation-state hackers could result in big losses and massive damages, because of the resources and time that attackers invest in their missions. This became clear in the most recently Russia-linked SolarWinds hack that targeted the software development stage and went undetected for several months after many organizations were breached. [12]

Protecting organizations' and governments' assets from nation-state cyber threats requires proactive, active, and reactive security postures, in addition to the deployment of multi-layered security strategies. For instance, this could include avoiding the usage of equipment made by vendors from the suspected nations with state-sponsored actors, investing in the human aspect of the security for the organization, through constant training and security awareness. Humans can become an easy target to be exploited. Additionally, with the studies and intelligence gathered from previous nation-state cyber-attacks, there are security frameworks that have been developed by security experts to reduce the attack surfaces of the organizations. These frameworks are not security tools, but just layouts of how effective security should be implemented. This article only highlights three of such frameworks, and it is worth mentioning that the proper implementation of these frameworks in organizations has tremendously reduced state-sponsored cyber-attacks.

NIST Cybersecurity Framework:

NIST Cybersecurity Framework defines five functions that should be implemented to track and secure an organization's assets and infrastructure. Each function acts as an implementation phase with specific requirements and practices. It is worth noting that this is just a framework and an organization should implement it in a way that meets the business requirements of the company. NIST defines five stages: Identifying, Protecting, Detecting, Responding, and Recovering. The first three stages of this framework highlight the proactive and active security postures that be well implemented to protect organizations from attacks or detect any attempted attack. The last two stages are proactive security postures which define how to respond to a security incident.

ATT&CK Matrix:

This is a knowledge-based model that works on adversarial-tactics and techniques based on real-world observations. This framework can be utilized as a foundation to develop specific threat-models and methodologies affecting the private-sectors, governments, and cybersecurity products and service-communities. ATT&CK Matrix emulates the initial access, execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, command, and control (C2), exfiltration, and impact, from the attacker's perspective. A proper implementation will in understanding the attackers and their techniques.

Cyber Kill Chain:

The Cyber Kill Chain framework is based on an Intelligence-driven Defense model to identify and prevent cyber-intrusion activities. It works by identifying the activities that the attackers must go through to accomplish their objectives and breaking that chain to disrupt the attackers' workflow. For a successful attack, attackers should completely progress through the attack stages defined by this model. Understanding the attackers' attack stages and breaking the chain between these stages will make it harder for the attackers to succeed. The attack stages defined by this framework are reconnaissance, weaponization, delivery, exploitation, installation, command, and control (C2), and action on objectives.

Conclusion

The emergence of Nation-state threat actors introduced a new security challenge in cyberspace, with developed and developing countries building and hardening cyber-forces and capabilities. We have witnessed what APT groups are capable of: from corporate espionage, political and governance interference, to trying to disrupt the military capabilities of other countries. With their sophisticated modes of operations and resources, nation-state cyber-threats have been successful in most of their hacking campaigns, and organizations are still struggling and having challenges in protecting their assets from the APTs. However, there are security measures and strategies that can be implemented to reduce the attack surfaces in the organization and reduce the success rate for most of the attacks from state-sponsored attackers.

References

1. Mueller, R. (2018). United States Grand Jury Indictment. Retrieved 28 January 2020, from https://www.justice.gov/file/1080281/download
2. CrowdStrike (2020). Crowdstrike Intelligence Report. Retrieved 8 March 2020, from http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf
3. Joske, A., & Jones, C. (2019). How China Uses Its Universities to Spy on America. Retrieved 19 March 2020, from https://nationalinterest.org/blog/buzz/how-china-uses-its-universities-spy-america-100557
4. F-Secure (2020). The Dukes 7 years of Russian cyberespionage. Retrieved 28 January 2020, from https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf
5. Australian Strategic Policy Institute (2020). China Defense Universities Tracker. Retrieved 19 March 2020, from https://unitracker.aspi.org.au/
6. FireEye (2020). [Report] Double Dragon: APT41, a Dual Espionage, and Cyber Crime Operation. [online] Available at: https://content.fireeye.com/apt-41/rpt-apt41/ [Accessed 28 Jan. 2020].
7. Cimpanu, C. (2019). Building China's Comac C919 airplane involved a lot of hacking, report says | ZDNet. Retrieved 5 February 2020, from https://www.zdnet.com/article/building-chinas-comac-c919-airplane-involved-a-lot-of-hacking-report-says/
8. Schwartz, M. (2013). China Tied To 3-Year Hack Of Defense Contractor. Retrieved 5 February 2020, from https://www.darkreading.com/risk-management/china-tied-to-3-year-hack-of-defense-contractor/d/d-id/1109795
9. Ottis, R. (2007). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. Retrieved 2 March 2020, from https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf
10. Zetter, K. (2014). An Unprecedented Look at Stuxnet, the World's First Digital Weapon. Retrieved 2 March 2020, from https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
11. Wray, C. (2020). Responding Effectively to the Chinese Economic Espionage Threat. Federal Bureau of Investigation. Retrieved 9 March 2020, from https://www.fbi.gov/news/speeches/responding-effectively-to-the-chinese-economic-espionage-threat
12. Microsoft Security (2021). Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers - Microsoft Security. Available at: <https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/> [Accessed 13 February 2021].
13. Rosenbaum, R. (2012). Richard Clarke on Who Was Behind the Stuxnet Attack. Retrieved 18 March 2021, from https://www.smithsonianmag.com/history/richard-clarke-on-who-was-behind-the-stuxnet-attack-160630516/
14. US 'launched cyber-attack on Iran weapons systems'. (2019). Retrieved 18 March 2021, from https://www.bbc.com/news/world-us-canada-48735097