Snode

Sovereign Security

The critical risks to global software supply chains

14 May 2021

www.snode.com
info@snode.com
+27 12 880 0989

Table of contents

Introduction

In the hyperconnected world of today, digital infrastructure and technology has reimagined the traditional notion of security and state sovereignty. Cyberspace has become fundamental for both governments and its citizens through one key function: access to information.

Information transference is a landscape for economics and civil discourse, while also being a battleground for war waged by nation-states, adversarial groups and autonomous actors (Ayers, 2016). As with any battle, not all parties follow the same rules of engagement.

The interconnection of global information infrastructure, technological trade and intelligence between nation states or intelligence agencies and technology providers has created a cavernous grey area between spying and war. Central to information warfare is that both state, military and civilian collateral is to be acquired at all costs; be it through intelligence alliances, subversion or espionage.

This paper will evaluate the ever-shifting cyber battleground of electronic surveillance - targeted at allies and enemies alike - and the manner in which it fuels political agenda, capital gain, social discourse, and catastrophic compromise of national security.

Commoditising intelligence and international espionage

Informational alliances and technological trade between governments, intelligence agencies and private companies has been a cornerstone of continental advancement for centuries. However, just last year, it was revealed just how deep subversion runs in the world's appetite for local and foreign intelligence.

For more than half a century, governments across the globe utilised a single company to keep their sensitive military communications and national intelligence a secret. Swiss company Crypto AG was deployed to develop code-breaking devices for America to use against enemies in World War II. Thereafter, Crypto AG became a dominant producer of encryption devices for decades to come, rolling out technology fit for the times: spanning metal gears and circuit boards, to silicon and software (Miller, 2020).

Throughout its history, Crypto AG sold technology to more than 120 countries, including India, Pakistan, Iran, Saudi Arabia, Italy, Libya, South Korea and Latin America. As a company that dealt in confidentiality, their best-kept secret was only revealed years later: Crypto AG was, in fact, owned by the CIA in partnership with West German intelligence agency, BND.

The intelligence partnership manipulated the company's hardware to decipher the codes that their customers used to transmit encrypted messages, well after the turn of the millennium. The operation monitored authoritarian regimes and manipulated international relations, preventing certain adversaries from acquiring weapons or technology that would give them an advantage, while ultimately maintaining the interests of the United States and its allies (Miller, 2020). Though Russia and China were never customers of Crypto AG, the CIA and BND gathered intel on their biggest adversaries by keeping tabs on other countries' dealings with Beijing and Moscow.

The Crypto AG intelligence coup transcended just the States and Germany; the intel garnered was used to the advantage of their allies. This revelation shone the spotlight on the pervasiveness of cyber espionage, where monitoring the encrypted communications of both allies and adversaries can be used for sovereign advantage.

The vested interest of state intelligence in cyber security

The Crypto AG case study was a foreshadowing of modern espionage; the extent and intricacy of the CIA's surveillance was just the start of an insatiable desire for global surveillance by world powers (Miller, 2020). This is not the first, nor last time that state intelligence firms have backed cyber security and defence technologies for national benefits and foreign reconnaissance.

State's investment in intelligence

As a nation that is almost always at war, Israel invests a substantial amount of capital and state support in technological innovation, particularly in the realm of cyber security and defence. Unit 8200, the cyber security arm of the Israeli Defence Forces, plays a fundamental role in developing Israel's technological prowess, resulting in the country boasting the highest concentration of startups per capita globally. Messaging app Viper and cloud computing service Wix originated after their founders completed their services for Unit 8200.

The operation's modus operandi is to consistently generate thousands of tech-savvy entrepreneurs to keep the country on the cutting edge of technology and cyber defence, by either founding their own companies or grooming them to occupy top positions in established ones (Valache, 2020). The organisation takes a grassroots approach to skills development, investing in coding and tech educational programmes, while recruiting promising students with analytical capabilities.

AI at the forefront of cyber defence

GCHQ, the United Kingdom's intelligence and security organisation, is currently investing in Artificial Intelligence to combat cyberattacks, identify state-backed disinformation and track criminal networks around the globe (Warrell, 2021). This expanded focus on cyber-offensive capabilities is a result of growing hostility and increasing security threats from China and Russia.

Through what has been touted as "good AI", GCHQ means to employ machine learning to support national security through various applications, based on the organisation's unprecedented access to the volume of data needed to train algorithms. These include machine-assisted fact checking to discredit deepfakes, automatically detecting and blocking botnets, finding malicious software and tracing it to its source and shutting down terrorist group communications (Warrell, 2021).

Artificial Intelligence employed under the guise of counterterrorism and eavesdropping on both allies and enemies is cause for concern, where the sensitive information of citizens is involved. What is the cost of civilians' privacy for state security?

Historic focus on hardware hacking

Hardware hacking has held centre stage in global security concerns for decades. After all, encryption hardware is potentially pervasive and devastating; access to internationally distributed hardware is lucrative for long-term intelligence mining - for both private companies and government.

In 2015, Lenovo was exposed for installing invasive marketing software on its laptops without the user's permission or knowledge (Khandelwal, 2015). The Chinese computer manufacturer pre-installed spyware on their machines which would transmit sensitive user information directly to the company. This is not the first time Lenovo has been accused of embedding tracking software within their hardware; in the year prior, their laptops were found to have housed Superfish malware and non-removable crap-software in two separate instances.

Likewise, it was revealed in 2017 that HP PCs and laptops contained a service named HP Touchpoint Analytics Client, a software that appeared on Windows machines as part of an update. This analytics service - which users did not opt into - constantly ran in the background to harvest user's data without consent, and this information was sent to HP daily (Humphries, 2017).

Motherboard manipulation with malicious intent

One of the most pervasive technology supply chain hacks in US history was uncovered in 2018, compromising up to 30 American conglomerates. In 2015, Amazon.com was looking to expand its Prime Video streaming service, and earmarked Elemental Technologies as a prospective partner to roll this out. Elemental developed software for compressing massive video files and formatting them for different devices. Elemental's repertoire included streaming the Olympic Games, communications with the International Space Station, and channeling drone footage to the CIA (Robertson & Riley 2018a). Their servers were also present in Department of Defense data centres, and in the onboard networks of navy warships.

As part of the company's due diligence into the prospective acquisition, Amazon Web Services brought on a third-party company to vett Elemental's security, particularly around the servers that their customers installed into their networks to manage video compression. Elemental acquired these servers from Super Micro Computer Inc., one of the world's largest suppliers of server motherboards. During their investigation, Amazon's third-party testers discovered a minute microchip - not much larger than a grain of rice - that was not a part of the hardware's original design.

Most disconcertingly, Elemental was just one of hundreds of Supermicro customers across the globe. During a three-year probe, US authorities discovered that the microchips enabled a remote attacker to establish a stealth doorway into any network that housed the adapted servers. Investigators believed that the microchips had been inserted by Supermicro's motherboard manufacturing sub-contractors in China. Other companies affected included a major US bank, government contractors, and most notably global tech giant, Apple, who ended their relationship with Supermicro the following year.

In statements issued in October of 2018, Amazon expressed that it was untrue that AWS knew about a supply chain compromise, an issue with malicious chips, or hardware modifications when acquiring Elemental (Robertson & Riley 2018b).

Software supply chain compromise

Software supply chain compromise is becoming more and more prevalent on the world's stage, it is far from a new phenomenon. By compromising the most insecure element of the software supply chain, a malicious actor has the ability to mine data, corrupt systems, or gain access to other parts of the network through lateral movement (Pritchard, 2021). Further to this, software is being exploited more frequently as attribution of the contamination is far more difficult, as one cannot quantifiably say who compromised the software in the first place.

Central to its success as an attack vector is that software vendors service many customers, meaning that a breach can compromise a multitude of organisations simultaneously. As such, it is pertinent that companies are selective about where their solutions come from in context to the critical nature of the environments into which the software is deployed. Untrustworthy technology choices have a potentially devastating impact on sovereign security.

In 2021, the gravity of supply chain risk was realised in what is being named the largest and most sophisticated software supply chain attack to ever hit the globe. The hacking campaign compromised Orion, an IT monitoring and management application, manufactured by SolarWinds Corp, giving hackers line of sight into thousands of companies and government offices that utilised the products (Heath, 2021).

Cyber security company FireEye was one of the first to discover that attackers had converted an element of Orion into a back door into their information technology systems that communicated with third-party servers (Pritchard, 2021). Dubbed "Sunburst", the trojanised malware gave threat actors access to email addresses and contact information, and the ability to eavesdrop on communications, destroy or alter data, and impersonate individuals within networks.

During the weeks thereafter, a multitude of technology corporations, Fortune 500 companies and government departments across the globe discovered Sunburst within their systems. These included the US Departments of Homeland Security, Treasury, Justice and Commerce respectively, as well as Mimecast, Microsoft, Deloitte and Intel. In total, the breach compromised as many as 18 000 SolarWinds customers.

It is believed that the Sunburst trojan first started to infiltrate global networks as far back as March 2020. Due to the extent and pervasiveness of the software compromise, it could be months, if not years, before the affected networks are secure again.

The attack has been linked to Russian state-sponsored cybercrime organisation APT29, though the Russian government denies responsibility for the campaign.

Instant messaging monitoring

Last year, popular Emirati messaging app ToTok came under fire as an undercover spying tool. Downloaded more than a million times from the Apple and Google Play app stores, its appeal lay in the easy and secure manner in which individuals could communicate by video or text, particularly in a country that restricts access to messaging services such as Skype and WhatsApp (Mazzetti, Perlroth & Bergman 2020).

In reality, ToTok was a shrewdly designed platform exploited by the United Arab Emirates government to monitor the conversations, locations, photographs, audio files and relationships of its users. The app's

privacy policy made no mention of end-to-end encryption, only that "we may share your personal data with group companies" - meaning that ToTok enabled the UAE government to convince millions of users to give out their most personal data for free.

Social media discourse and information warfare

The digital arms race of today transcends just software. Social media is the battlefield political warfare, with disinformation being the weapon of choice. The most prevalent example is the subterfuge Russian intelligence deployed through social media to polarise American political perception and sway the 2016 Presidential Election. In order to spread false and distorted information and influence campaigns, Russian-funded troll factories created racially and politically divisive social media groups and pages, developed fake news articles and manipulated conversations online to build political animosity within America (Summers, 2018). In tandem, UK-based political consulting firm Cambridge Analytica utilised Facebook for political voter surveillance to influence Ted Cruz' 2016 US Republican nomination.

Evolved false flag strategy

In 2017, documents detailing the CIA's most sophisticated software tools and techniques for international espionage were exposed by Wikileaks, in the largest leak of classified information in US history. Dubbed as Vault 7, the documents showcased a highly technical range of tools, including instructions for compromising a wide range of common computer tools for spying purposes, including Skype, Wi-Fi networks, PDF documents and popular antivirus software (Shane, Rosenberg & Lehren, 2017).

A large proportion of these documents focused on the agency's anti-forensics tools, referred to as Marble Framework. In order to hamper forensic investigators, this code is designed to make it easier for those writing malware to disguise who created it (Burgess, 2017). The technology's capabilities include the ability to develop malware in another spoken language, such as Mandarin, Russian, Korean or Arabic. This means that the malware can appear to have originated from another country.

This is not dissimilar to false flag strategy, a tactic that was first employed during naval warfare in the 16th century. During times of combat, a vessel would fly the flag of a neutral or allied country in order to disguise its intent and reveal its true flag before attacking its targeted ships.

This tactic has been replicated in modern cyber warfare, where a terrorist act is committed with the purpose of disguising the original source and holding another government responsible for the aggression. This act, committed by private organisations or covert government agencies is executed with insidious intent: to exert domestic repression, or retaliate with military aggression.

The modern-day art of war

All warfare is based on deception; the tactics employed are as old as time itself, only the tools have changed. In the ever-changing face of war, there is no camaraderie in the world of information espionage; the global desire for surveillance means no one is immune to covert monitoring.

The best defence for sovereign security is a central conduit of intelligence that is not influenced by state or national intelligence. Though complex, the permeable nature of security borders must be made more rigid to protect the critical infrastructure and privacy of the public, and private entities.

About Snode Technologies

Snode is a cyber defence company focused on making the unknown known. Snode is driven by excellence and the desire to tackle client challenges with bleeding-edge cyber technology.

Snode has over 80 global points of presence, protecting large industrial, agricultural, telecommunications and financial infrastructures.

Authors

Nithen Naidoo

CEO and Founder of Snode Technologies

Nithen Naidoo is the CEO and founder of Snode Technologies. As a cyber security evangelist, with over 20 years of experience, Nithen provides cyber defence solutions globally, and most recently was recognised by the prestigious AfricArena tech accelerator as an Emerging Entrepreneur of 2021. Nithen is also a sought-after public speaker.

Snode Technologies, a cyber defence firm based in Centurion, South Africa, has been a finalist and winner of some of Africa's most prestigious innovation awards, most recently, an overall winner at the SA Innovation Summit 2020 and the MEST Africa Challenge 2019. Snode was also listed, by Slingshot (Singapore), as one of the (2020) Top 100 Deep Tech innovations globally.

Lauren Crooks

Lead Strategist at Coalition Communications

Lauren Crooks is a seasoned communications strategist and copy-writer, and has over a decade of experience in communications and marketing. Lauren has developed a dynamic portfolio in meaningful and engaging brand architecture, and cutting-edge through-the-line strategy in the realms of technology, logistics, manufacturing and mining.

Lauren holds an Honours degree in Psychology.

References

Ayers, C.E. (2016). Rethinking Sovereignty in the Context of Cyberspace. The United States Army War College.

Burgess, M. (2017). WikiLeaks drops 'Grasshopper' documents, part four of its CIA Vault 7 files. Wired. Retrieved from: https://www.wired.co.uk/article/cia-files-wikileaks-vault-7

Heath, B. (2021). SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president. Reuters. Retrieved from: https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R

Humphries, M. (2017). HP accused of quietly installing spyware on Windows PCs. PC Magazine. Retrieved from: https://sea.pcmag.com/news/18409/hp-accused-of-quietly-installing-spyware-on-windows-pcs

Khandelwal, S. (2015). Lenovo caught (3rd Time) pre-installing spyware on its laptops. The Hacker News. Retrieved from: https://thehackernews.com/2015/09/lenovo-laptop-virus.html

Mazzetti, M., Perlroth, N., & Bergman, R. (2020). It seemed like a popular chat app. It's secretly a spy tool. The New York Times. Retrieved from: https://www.nytimes.com/2019/12/22/us/politics/totok-app-uae.html

Miller, G. (2020). The intelligence coup of the century. The Washington Post. Retrieved from: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/

Pritchard, S. (2021). Software supply chain attacks – everything you need to know. Portswigger. Retrieved from: https://portswigger.net/daily-swig/software-supply-chain-attacks-everything-you-need-to-know

Robertson, J. & Riley, M. (2018a). The Big Hack: how China used a tiny chip to infiltrate U.S. companies. Bloomberg. Retrieved from: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Robertson, J. & Riley, M. (2018a). The Big Hack: Statements From Amazon, Apple, Supermicro, and the Chinese Government. Bloomberg. Retrieved from: https://www.bloomberg.com/news/articles/2018-10-04/the-big-hack-amazon-apple-supermicro-and-beijing-respond

Shane, S., Rosenberg, M., & Lehren, A.W. (2017). WikiLeaks releases trove of alleged C.I.A. hacking documents. The New York Times. Retrieved from: https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html

Summers, T. (2018). How the Russian government used disinformation and cyber warfare in 2016 election – an ethical hacker explains. The Conversation. Retrieved from: https://theconversation.com/how-the-russian-government-used-disinformation-and-cyber-warfare-in-2016-election-an-ethical-hacker-explains-99989

Valache, C. (2020). Israel's Unit 8200, a conveyor belt of high-tech startups. Interesting Engineering. Retrieved from: https://interestingengineering.com/israels-unit-8200-a-conveyor-belt-of-high-tech-startups

Warrell, H. (2021). UK spy agency to use AI against cyber attacks and state actors. Financial Times. Retrieved from: https://www.ft.com/content/2b32d454-1cbe-48e7-a12c-fdc2069b6d5c