RMC

Risk Mitigation Consulting Inc.

Intelligence and Analysis Division

WHITE PAPER SERIES

The Security Implications of Foreign Hardware/Software

INTENT

This white paper is designed to provide an in-depth analysis of relevant, publicly available information on threat and hazard events/trends and their potential impacts to the interests of the United States, both at home and abroad. This product is not intended to be an all-encompassing assessment of the subject, rather, it provides a brief overview to provide the reader with situational awareness regarding topics with which they may not be familiar.

The Security Implications of Foreign Hardware/Software

Introduction

The presence of foreign technologies (to include both hardware and software products) are widespread throughout the U.S. and the global economy. However, foreign government-owned firms (as well as those with government ties) remain a serious security concern to consumers due to the potential for malicious activity, such as the installation of backdoors, malicious code, and surveillance concerns. In particular, foreign government-owned or government-affiliated firms from U.S. adversaries such as China and Russia have come under scrutiny in recent years due to the potential for espionage or other forms of malicious cyber activity. This paper will examine the current security environment related to these firms; the ways in which they can exploit various hardware and software products for nefarious purposes; as well as a number of select case studies involving security concerns associated with particular foreign government-owned or government-affiliated firms.

Security Concerns Associated with Foreign Hardware/Software

Potential Motives of Foreign Firms

Foreign firms may have a variety of motives to use hardware/software for nefarious purposes. However, this paper will examine two primary motivating factors: foreign firms that are owned either wholly or in part by a government entity; and foreign firms that have apparent or alleged ties to government entities. Foreign firms that are government-owned nor government-affiliated are not inherently a security threat, however, firms that are government-owned or have affiliations with military or security services may have a greater willingness to engage in surveillance or other malicious activities at the behest of governmental authorities. These malicious activities could include cyberattacks or other exploitable actions using technological means.

For example, suppose that Software Company X was owned (either wholly or in part) by a foreign government that is hostile/adversarial to the U.S., or, alternatively, that its CEO is a former high-ranking intelligence official of said government. Additionally, suppose that Software Company X's products have been widely adopted by U.S. consumers (to include individual users, corporate entities, as well as government agencies). Seeing an opportunity for surveillance/intelligence collection purposes, the foreign government could direct Software Company X (which is ostensibly sympathetic to the foreign government's objectives) to monitor U.S. users' activity and pass exploitable information on to the country's intelligence agency. Moreover, in a time of conflict, the foreign government could direct Software Company X to use its products as a vector for malicious code in a cyberattack against the U.S., or it could plant similar "sleeper" code in less turbulent times that could be "activated" during future conflicts. These examples are not all-encompassing, rather, they highlight just a few reasons why foreign government-owned or government-affiliated technology firms ought to be cause for concern.

Potential for Malicious Cyber Activity

Although full-scale cyberwarfare between nation-states has not yet occurred, a number of smaller-scale cyberattacks have been documented in recent years. Foreign government-owned or government-affiliated firms may utilize their own hardware and software as a to carry out such attacks. These firms' hardware or software products could contain malicious code (either running actively, or programmed as a "sleeper" option, as in the aforementioned example), backdoors, or other deliberately exploitable features. Additionally, foreign hardware and software could be utilized as a potential vector or "stepping stone" for other types of state-sponsored cyber activity.

Additionally, foreign governments could potentially compel firms to manipulate software and hardware products related to supervisory control and data acquisition (SCADA) systems. SCADA systems are computer systems "that are employed to control and keep track of equipment or a plant in industries like water and waste control, telecommunications, energy, transport, and oil and gas refining."[1] Critical infrastructure is likely a highly appealing target in times of conflict or crisis, and foreign government-owned or government-affiliated firms may be in a unique situation to access and/or affect such infrastructure via SCADA systems. Some high-profile examples of cyberattacks against SCADA systems include the Stuxnet worm (which reportedly targeted Iranian nuclear facilities in a manner that destroyed centrifuges used for the refining of uranium), as well as the December 2015 cyberattack against Ukraine's power grid by presumed Russia-linked actors.[2,3]

Potential for Surveillance

As will be seen in the case studies detailed below, concerns remain high regarding the potential for surveillance by foreign government-owned and government-affiliated firms. A number of high-profile incidents in recent years regarding foreign hardware and software products have emerged, in some cases leading to U.S. government bans on the procurement/use of such products for official purposes. Despite such bans, these products remain widely used by civilians and corporations, while surveillance concerns remain. In many cases, these foreign firms vehemently deny the existence of malicious intent, or any capabilities to carry out any surveillance activities. However, many common hardware/software products have the capabilities to carry out surveillance (or can be modified to do so), and foreign firms that are government-owned or government-affiliated may have a motive to do so.

For example, hardware products such as personal computers (PCs) or cell phones are widely used by government and civilian users alike, and often contain or transmit data that is personal; proprietary; commercially valuable; or in some government applications, may include data that is considered classified. These hardware products typically operate a variety of software programs, which may also be exploitable. A foreign government-owned or government-affiliated firm may exploit such hardware or software with the goal of surveilling the products' end users in pursuit of the aforementioned categories of data. Personal data could be exploited for blackmail or other espionage-related purposes, while proprietary/commercially valuable data could be exploited for economic purposes. However, the collection of sensitive and/or classified data is of the highest concern, due to the potential for serious national security impacts.

Case Studies

Overview

The case studies detailed below vary somewhat in nature, and primarily focus on the potential for surveillance activities. It should be noted that there is not a well-documented history of foreign firms engaging in cyberattacks at the behest of their own government, although the potential for such activities currently exists and may potentially increase in the coming years as cyberwarfare becomes a more prevalent activity among states. Additionally, it should be noted that in the case studies detailed below, there is limited information at best to suggest that such firms are engaging in malicious activities such as surveillance. Still, the concerns regarding such activities have risen to a level where the U.S. government has taken legislative or other policy actions to prevent such hardware or software from being procured for/used in official U.S. government activities.

Huawei/ZTE

The U.S. government has repeatedly expressed concerns regarding Huawei and ZTE (both of which are prominent Chinese telecommunications firms) in recent years. Both firms manufacture a wide range of telecommunications hardware, from individual mobile devices to equipment used in telecommunications networks. These devices may provide a platform for surveillance or other malicious activities. Additionally, both firms have known ties to the Chinese government. Huawei's founder is a former engineer of China's People's Liberation Army, although the company is purportedly employee-owned, while ZTE's controlling shareholder is a Chinese state-owned corporation.[4,5] Moreover, a 2012 report by the U.S. House Select Permanent Committee on Intelligence contends that under Chinese law, "ZTE and Huawei would likely be required to cooperate with any request by the Chinese government to use their systems or access for malicious purposes."[6] These factors provide a number of potential motives for Huawei and ZTE to engage in malicious activities such as surveillance.

In 2018, the U.S. government engaged in multiple actions to mitigate the potential threat from Huawei and ZTE. In May 2018, the Pentagon banned Huawei and ZTE products from being sold in stores located on U.S. military installations, although the action did not necessarily prevent service members from owning such devices or acquiring them through other means. More notably, lawmakers added a bipartisan provision to the 2018 National Defense Authorization Act (the legislation that appropriates funding for the Department of Defense) to prohibit procurement of Huawei/ZTE products for official U.S. government purposes.[7] Additional policy actions against Huawei, ZTE, and other Chinese firms may be implemented in the near future as U.S.-China tensions persist.

Kaspersky Labs

Kaspersky Labs, a Russian cybersecurity firm that manufactures software products such as antivirus programs, has also been the subject of espionage allegations by the U.S. and other governments. A 2015 investigative report on Kaspersky noted that its founder "was educated at a KGB-sponsored cryptography institute, then worked for Russian military intelligence," while also alleging that some Kaspersky employees have close ties to Russian military/intelligence services, even aiding in some investigations using data gathered using Kaspersky's software.[8] In 2017, the U.S. government banned the use of Kaspersky's antivirus software among federal agencies due to security concerns. A statement by the Department of Homeland Security expressed concern "about the ties between certain Kaspersky officials and Russian intelligence and other government agencies, and requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting Russian networks." A few months prior to the ban, the General Services Administration (the U.S. government agency in charge of government procurement) had removed Kaspersky from its list of approved vendors.[9]

In order for antivirus software to function effectively, such software must have extensive access to a computer's contents, settings, etc… in order to scan for abnormal activity. This level of access could potentially provide Kaspersky Labs with a wide variety of sensitive U.S. government information, which, if passed on to Russian authorities, may be of intelligence value. Moreover, U.S. corporations running Kaspersky antivirus software could be risking the loss of trade secrets and other economic information. Individual consumers' information would also be at risk, and users with sensitive employment or ties to high-value individuals could potentially expose themselves to the risk of blackmail.

Lenovo

Ongoing U.S.-China tensions and security concerns surrounding Huawei and ZTE have also led to increased scrutiny of other Chinese technology firms. A recent report commissioned by the U.S.-China Economic and Security Review Commission called Lenovo (a major manufacturer of computers, smartphones, and smart televisions, among other products) a "cyberespionage risk." The authors of the report noted that the Chinese government could exploit Lenovo to conduct surveillance on (or otherwise compromise) U.S. government computer systems due to Lenovo's previous links to "Chinese state-led cyberespionage efforts."[10]Additionally, this is not the first time Lenovo has been scrutinized by U.S. authorities. In 2006, the U.S. Department of State abandoned plans to purchase hundreds of Lenovo computers for a classified computer network due to political pressure relating to espionage concerns.[11] However, several analysts at the time noted that it was extremely difficult to procure computer hardware that did not have at least some foreign origin and argued that such security concerns were exaggerated.

Outlook

The proliferation of foreign hardware and software throughout the U.S. and the global economy will inevitably lead to security concerns, particularly when foreign technology firms are government-owned or government-affiliated. Although there is little evidence available publicly to suggest that firms such as Huawei, ZTE, Kaspersky, or Lenovo have engaged in surveillance or other forms of malicious cyber activity due to their known or alleged ties to foreign governments, the U.S. government has repeatedly taken policy actions to mitigate potential security threats from these and other firms. Still, concerns remain, not only within the government sector, but also among commercial entities and individual consumers alike. The aforementioned firms (in addition to countless others) continue to possess an impressive capability to conduct surveillance and other forms of malicious cyber activity via their hardware and software products. This capability is unlikely to be diminished anytime soon, as factors such as globalization, economic competition, and consumer preferences take precedence over underlying security concerns.

Source List

1. Techopedia. *Supervisory Control And Data Acquisition (SCADA)*. Retrieved 31 January 2019.
2. Wired. *An Unprecedented Look At Stuxnet, The World's First Digital Weapon*. 03 November 2014.
3. British Broadcasting Company (BBC). *Hackers Behind Ukraine Power Cuts, Says US Report*. 26 February 2016.
4. CNN. *Huawei's Founder Praises Trump And Denies Claims His Company Spies For China*. 16 January 2019.
5. CNN. *ZTE Is Now Center Stage In The US-China Trade Fight*. 10 May 2018.
6. United States House of Representatives, Permanent Select Committee on Intelligence. *Investigation Of The Security Threat Posed By Chinese Telecommunications Companies Huawei And ZTE*. 13 September 2012.
7. The Hill. *Lawmakers Target ZTE, Huawei In Defense Bill*. 07 June 2018.
8. Bloomberg Businessweek. *The Company Securing Your Internet Has Close Ties To Russian Spies*. 19 March 2015.
9. The Washington Post. *U.S. Moves To Ban Kaspersky Software In Federal Agencies Amid Concerns Of Russian Espionage*. 13 September 2017.
10. Durham Herald Sun. *Lenovo Called "Cyberespionage Risk" By D.C. Consultants*. 26 April 2018.
11. NetworkWorld. *Security Experts: U.S. Government's Lenovo Ban Misguided*. 26 May 2006.