CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

The Growing Cybersecurity Risk in Software Supply Chains

by Sam Cohen

August 2019

POLICY PERSPECTIVE

THE GROWING CYBERSECURITY RISK IN SOFTWARE SUPPLY CHAINS

by Sam Cohen

August 2019

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Prepared for the Canadian Global Affairs Institute
1800, 421 – 7th Avenue S.W., Calgary, AB T2P 4K9
www.cgai.ca

ISBN: 978-1-77397-081-3

Canadian businesses and government agencies are facing increased cybersecurity risk from compromising situations occurring throughout their software supply chains. Advanced, well-funded and dedicated threat actors no longer need to directly bypass or defeat security countermeasures such as external firewalls. Instead, they can compromise third-party software suppliers and products that will eventually be deployed within a targeted corporate or government enterprise. CrowdStrike, a leader in the cybersecurity and endpoint protection field, conducted a survey in 2018 which questioned 1,300 IT security professionals about the risks and impacts of software supply chain attacks. More than 66 per cent of survey respondents indicated that their organization had experienced a software supply chain incident in the last 12 months, which on average incurred a financial cost of US$1.1 million. The organizations impacted by these attacks included government bodies and high-tech research and manufacturing stakeholders in countries such as Canada, the United States, Japan and Germany.

Improvements in perimeter defences and network security have forced malicious actors to become creative with how they introduce malware into a target environment. The result has been increased exploitation of trusted relationships between an organization and its outsourced software providers, which can sometimes be smaller companies with weaker cybersecurity practices. Since many vendors try to move their product to market as quickly as possible to increase financial returns or to deliver improved products to customers in a timely manner, there can be a substandard implementation of safe software development lifecycle (SDLC) procedures – including a lack of routine code vulnerability analysis. This creates an opportunity for an attacker to embed malware into a software package without the vendor noticing.

For example, a criminal group can leverage a spear phishing email attack to entice an employee at one of these vendors to interact with a malicious attachment or they could recruit a company insider to engage with a malicious website. The result can be the unintentional or intentional download of a suspicious file that may allow the attacker to begin compromising information systems, escalating network access and functionality privileges, or locating additional vulnerabilities on the network. With greater interactive control and awareness of any countermeasures, an attacker could deliver tailored code into the software provider's development environment – code with potentially unique properties capable of masking itself from detection tools.

From the customer's perspective, they could be receiving a software product or update from their normal supplier as part of business-as-usual operations. In reality, this could be the first stage of a complex attack where malicious code has already been added to a product and can ride along an installation and execute in the background of a device or server. Without adequate cybersecurity posture to detect these attacks or secure SDLC practices to verify development integrity, a poorly defended software vendor is likely to increase a consumer's cyber-risk exposure.

Supply Chain Risk Management

Traditional approaches to supply chain risk management (SCRM) have centred on tracking the integrity of manufacturing and distribution of physical products, such as electronic hardware. Organizations and governments want to ensure that the physical equipment they are receiving is not counterfeit, has not been maliciously tampered with or damaged, and meets the technical specifications outlined in purchase contracts. From a software perspective, these core practices and objectives of SCRM are still relevant, but many new technical, legal and policy-based challenges are emerging.

For example, the popular use of open-source code libraries combined with the use of in-house proprietary application development creates a complex software lifecycle in which security and vulnerability assessment are difficult – particularly if the use of the open-source code was logged incorrectly or not tracked at all. In many instances, companies that either directly use open-source code or indirectly leverage open-source resources through a vendor's software program do not receive notifications or actively track updates and vulnerabilities for that open-source information. This can result in a gradual build of cyber-risk across an enterprise without security or IT teams even realizing it.

Malicious actors are well aware of the wide use of open-source code projects and often track their developments in real time to see what updates are occurring and which users may be using the code in their company's own development environment. For example, GitHub, which is a website and cloud-based service that helps developers store, track changes and manage their code – often in an open-source fashion—is a routine destination for hackers to conduct reconnaissance activities. Mark Curphey, CEO of SourceClear, a startup focused on securing open-source software for corporate developers, says that hackers will observe GitHub users contributing to certain projects and monitor what problems or functionality the code may have. With this knowledge, hackers can learn of a weakness in that individual's company, their in-house applications currently being built or software products they are developing for commercial resale. All of these avenues may augment an attacker seeking to insert malicious code at a later date into a software package that will eventually be deployed into a target environment.

Digital Certificates

From the technical side, software supply chain attacks are extremely difficult to detect and mitigate, largely because attackers disguise their malicious code under the validity of an authentic and secure product. Software updates and products typically have an associated digital certificate that communicates to customers that what they are downloading is not an altered or fake product – such as one that could have been created maliciously to confuse the customer. Essentially, business or government customers interpret valid certificates as a cryptographic guarantee of the trustworthiness of a piece of software. However, if the executable files in an update or a new product are infected before being digitally signed, the result can be a piece of software with embedded malicious code that appears safe for running on computer systems.

Candid Wueest, principal threat researcher with Symantec's Global Security Response Team, explains that "This attack is very, very stealthy and difficult to detect until it's running – and even then, you might not discover it." Matt Harley, VP of intelligent engineering at cybersecurity firm FireEye, reinforced this claim during his speech covering software supply chain risks at the 2018 International Cyber-Risk Management Conference (ICRMC) in Toronto. He noted that "Because an actor infects the software as it's being built, the process is essentially vendor source code, malware fused together, and then signed. So now, when you go to run that software or that app on your PC, it's signed, it's going to look good." These statements demonstrate the significant technical challenges corporate and government cybersecurity policies will need to address as threat actors continue to become increasingly sophisticated and creative with their vendor-based attack vectors.

A National Security Risk

While much of the current supply chain risk discussion in the U.S, Canada, Britain and other allied countries has focused on the challenges of guaranteeing security for the rollout of a new national 5G telecommunication hardware backbone, the risk from software poses an equally pressing issue to the telecom sector and to all major businesses across the country. CSE Canada, the country's leading agency for signals intelligence and national cybersecurity operations, dedicated a specific section in the 2018 "National Cyber Threat Assessment" just to supply chain risks. They explained that since 2013, on the topic of telecommunication supply chains, the agency has blocked a range of hardware, software and steady-state services that would have compromised the sector's integrity. The same section highlights that foreign governments have targeted Canadian technology and defence corporations to advance their national interests by exploiting the trusted relationships these businesses have with their software vendors and other partners throughout supply chains.

Foreign intelligence agencies and international cyber-criminals have targeted the software supply chains linked to governments and companies operating in the high-tech manufacturing and IT space, particularly those that interact with or service critical infrastructure. For example, the U.S. National Counterintelligence and Security Center released a report in 2018 detailing foreign government economic espionage activities in cyberspace across America and in allied countries. The report stated that "Hackers are clearly targeting software supply chains to achieve a range of potential effects to include cyber espionage, organizational disruption, or demonstrable financial impact." It also adds that "Software supply chain infiltration has already threatened the critical infrastructure sector and could threaten other sectors as well."

Software Supply Chain Compromises in the Wild: CCleaner Example

In September of 2017, Cisco's Talos Security Intelligence and Research Group, made up of leading threat researchers, discovered that the widely used software product CCleaner had been

maliciously altered by hackers and was being actively downloaded by a significant portion of the product's customer base. CCleaner software is a long-established system cleaner that can locate and remove potentially unwanted files and invalid Windows registry entries from a computer. CCleaner was initially developed, maintained and distributed by a company called Piriform, which was later wholly purchased by Avast, a Prague-based anti-virus firm. Avast maintains that the attackers infiltrated CCleaner's development environment while the rights still belonged to Piriform. Nevertheless, Cisco's Talos team reported that "For a period of time, the legitimate signed version of CCleaner [version] 5.33 being distributed by Avast also contained a multi-stage malware payload that rode on top of the installation of CCleaner." The scale of the incident was significant, as at the time of Avast's purchase, CCleaner had 130 million users, with 2.27 million ultimately downloading the files that were maliciously altered in the supply chain (i.e., while in development).

Nearly 1.7 million copies of the malware attempted to beacon back to the criminal group's command-and-control servers. Any victim domains that resembled a domain of a high-profile technology company or IT supplier were then automatically targeted for a second stage attack – which ultimately delivered additional malware to 40 computers. Avast confirmed that among those 40 computers were corporate devices at Samsung, Sony, Asus, Intel, VMWare, O2, Singtel, Gauselmann, Dyn, Chunghwa and Fujitsu.

Software Bill-of-Material (SBoM) as One Targeted Solution

In addition to well-developed cybersecurity strategy, procedures and tooling at the enterprise and vendor level, there is growing support for the use of software bill-of-materials (SBoMs) to increase resiliency against supply chain compromises. SBoMs aim to increase transparency into an organization's internal and external software development. Companies, government departments or organizations using external code libraries in addition to internal application development would be able to maintain an up-to-date list of key components and subcomponents included in any given piece of software within their IT environment. The benefit, at least theoretically, is clear: SBoMs would enable IT and security staff to quickly and proactively respond to newly listed vulnerabilities by identifying exactly which versions of deployed software on which devices – and what granular segments of that software – require patching or an update. SBoMs would also enable greater support for other cyber-risk management practices, such as efficiently tracking whether a piece of software is using any outdated or old components that are no longer being updated. This can remove commercial risks from IT procurement processes, enable greater management of software licensing and reporting requirements – which is already an active legal application of SBoMs – and reduce overall visibility challenges commercial software deployments often produce for IT security professionals.

Management of supply chain integrity and security challenges across hardware and software product acquisition lifecycles is becoming a key segment of daily business operations. Government agencies and businesses across Canada need to align appropriate industry and

government stakeholders to develop a framework for how SBoMs or other alternative approaches to software supply chain security can be implemented.

About the Author

Sam Cohen *is an incoming cybersecurity consultant with Deloitte's Toronto Risk Advisory Group. He previously worked with the Telecommunication Industry Association (TIA) in Washington, D.C. as a federal cybersecurity policy intern, and recently completed an M.S. in Defense and Strategic Studies at Missouri State University's Washington, D.C. campus and a certificate in cybersecurity strategy (IT security concentration) at Georgetown University.*

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including (in partnership with the University of Calgary's School of Public Policy), trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.