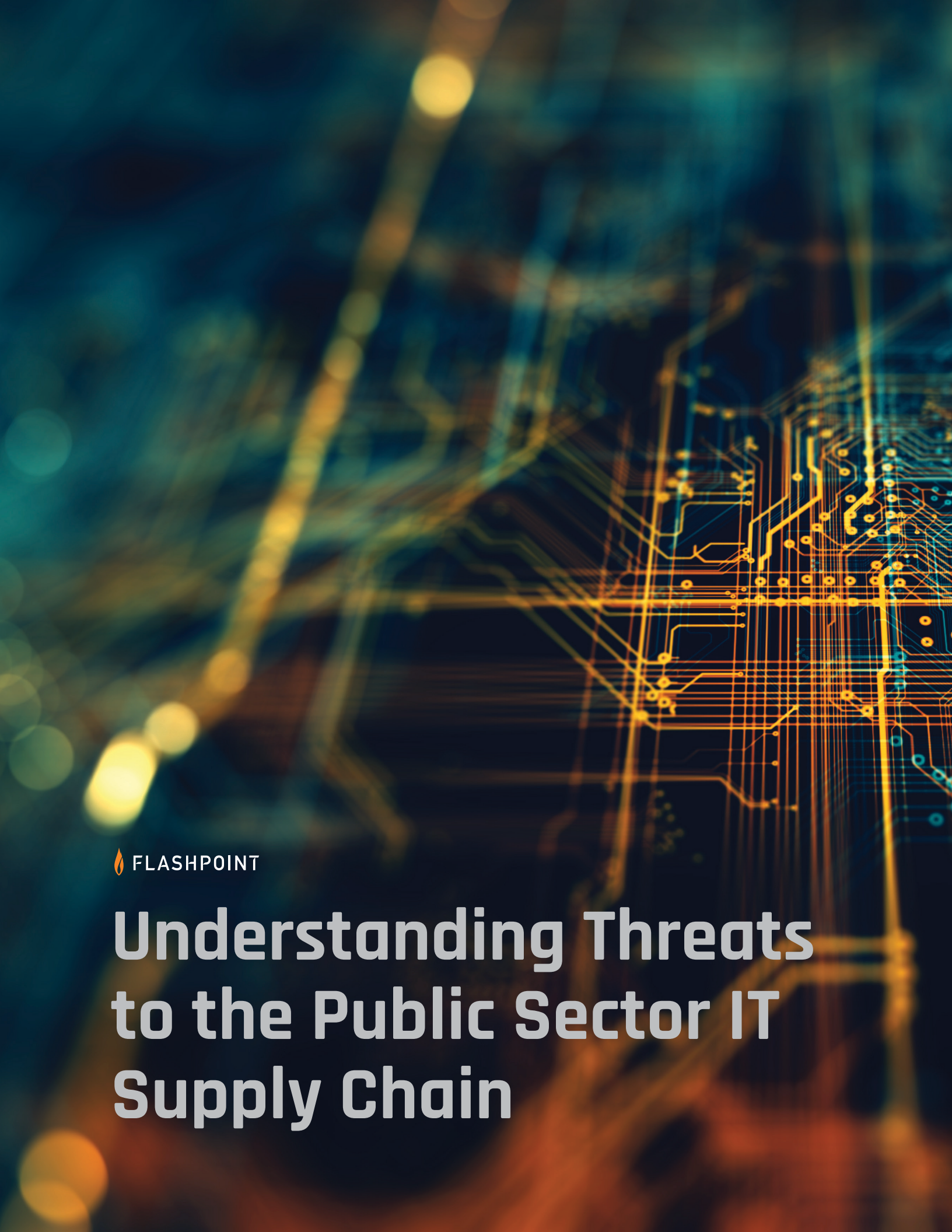

FLASHPOINT

Understanding Threats to the Public Sector IT Supply Chain

Understanding Threats to the Public Sector IT Supply Chain

ABSTRACT

The U.S. government's software and hardware supply chain is a complex and globally sourced entanglement of code and components from third-party manufacturers and service providers—some from less than amicable diplomatic and economic partners such as China. Often a mission-critical application or server is sewn together with components sourced from multiple providers and developers, making it untenable for a security manager to properly audit for interdiction along any stop of the supply chain.

This paper intends to examine the information security risks innate to the public sector IT supply chain for software and hardware, and their effect on the integrity and availability of federal IT systems and data. It will also enumerate the various standards and impending bills governing the security of the public-sector supply chain.

INTRODUCTION

The U.S. government's software and hardware supply chain is a complex and globally sourced entanglement of code and components from third-party manufacturers and service providers—some from less than amicable diplomatic and economic partners such as China. Often a mission-critical application or server is sewn together with components sourced from multiple providers and developers, making it untenable for a security manager to properly audit for interdiction along any stop of the supply chain.

This paper intends to examine the information security risks innate to the public sector IT supply chain for software and hardware, and their effect on the integrity and availability of federal IT systems and data. It will also enumerate the various standards and impending bills governing the security of the public-sector supply chain.

CRITICAL PUBLIC-SECTOR SERVICES, SYSTEMS IN CROSSHAIRS

Supply chain interdictions have been blamed for a number of attacks that have brought critical services to a standstill. Attackers who manage to introduce themselves into the software or hardware supply chains can exploit known or unknown weaknesses at a provider, thus injecting attacks at scale, or targeting specific entities known to be partnered with a provider. The result for a public-sector agency can be disastrous economically, or at a national security level.

Perhaps the most notorious and most recent supply chain attack is NotPetya. The attackers behind NotPetya spread wiper malware in June 2017 via a legitimate software update service belonging to Ukrainian financial software provider M.E. Doc. Computers grabbing the malicious update were infected with the wiper malware, which cripples the master boot record, bricking them instantly at a hardware level. Systems belonging to major government entities and private-sector enterprises, primarily in Ukraine, but also across Europe and Russia, were crushed permanently.

Earlier in 2017, CCleaner, a software optimization and maintenance tool for Windows machines, was backdoored via an automated update. System information was collected by this malicious update and sent to an attacker-controlled server. If certain domains were reporting back to the attackers, a second-stage payload was launched, leading to speculation this was an espionage attack.

Fears about supply chain cybersecurity risks were raised again in October when a controversial Bloomberg article alleged that operatives from China had managed to get backdoored chips onto motherboards manufactured by SuperMicro, a chip and hardware provider whose equipment is ubiquitous in servers, embedded computers, and mobile devices. Backdoor access to innumerable devices is an intimidating surveillance opportunity for a nation-state, though the veracity of the *Bloomberg* article has yet to be confirmed after strong denials from not only SuperMicro, but also Apple, Amazon, and others who claimed to have never found malicious chips on their devices.

Nonetheless, the *Bloomberg* article caused security managers and other executives to scramble in short

order looking for Super Micro chips among an army of servers and other hardware inside enterprises worldwide. Lawmakers on Capitol Hill demanded answers of Super Micro, and skeptical pundits questioned the bevy of anonymous sources backing up the Bloomberg report.

WHEN THE SUPPLY CHAIN EQUALS COMPLEXITY

Perhaps that's the one positive outcome here: a renewed focus and illumination of the risks posed by infiltrations, in particular to the public-sector supply chain. The U.S. government's information technology supply chain is the perfect representation of complexity, with each agency bound to maintain the availability and integrity of its systems while balancing a fragile train of software and hardware providers and other resources that make up the IT supply chain.

Any soft spot exposes critical systems to attack by unfriendly elements to the U.S., whether the impact targets agencies responsible for national security such as the Departments of Defense or Homeland Security, or something seemingly as benign as the Office of Personnel Management (OPM), which in 2015 suffered a catastrophic loss of personal information belonging to millions of current and former federal workers, including security clearance information.

The risk is deemed unacceptable by the U.S. government. Any interdiction of an IT system's development life cycle can have devastating consequences. The General Accounting Office in July released a report that identified a representative list of IT supply chain-related threats that includes:

- installation of intentionally harmful hardware or software (i.e., containing "malicious logic");
- installation of counterfeit hardware or software;
- failure or disruption in the production or distribution of critical products;
- reliance on malicious or unqualified service providers for the performance of technical services; and
- installation of hardware or software containing unintentional vulnerabilities such as defective code.

The manifestation of any of these types of attacks could impact not only the confidentiality and availability of critical systems and services, but also could negatively impact national security. A rogue insider, or exploitation of a vulnerability at any stop along the supply chain could introduce malware or exploits that could allow an adversary access to, or control of, a critical federal system. Further adding complexity to this scenario is the lack of visibility an agency may have beyond suppliers and manufacturers it directly deals with. Parts and code could be sourced from third parties in business relationships with those direct contacts, but a buyer on the federal might have no insight into the supply chain of its direct suppliers.

As a result, servers and endpoints inside agencies nationwide are likely being sourced from a global supply chain that can contain "multiple tiers of outsourcing," according to the July GAO report. Manufacturers from China, Malaysia, Singapore, Europe, South America, and North America can source components for workstations, notebooks, networking gear, telecommunications

equipment, servers and printers. One notebook, the GAO points out, could have its motherboard sourced from Taiwan, processor from any one of 10 countries, and memory and disk drive from a dozen locations.

It's complexity personified.

ESSENTIAL REGULATORY GUIDANCE AND OVERSIGHT

Federal agencies must, under the Federal Information Security Modernization Act of 2014, spell out and document information security programs, defining not only how to securely operate federal systems, but also how information security is addressed throughout the development and procurement lifecycles. The National Institute for Standards and Technology (NIST) has been directed to provide cybersecurity standards to agencies, while the Department of Homeland Security has oversight. Agencies have three key NIST resources at their disposal with regard to supply chain and procurement security.

NIST SP 800-39 is an overarching publication that explains how federal agencies should manage information security risk to organizational operations, assets, individuals, and the country. The recommendations are intentionally vague and non-prescriptive, but nonetheless address supply chain risks to be assessed during evaluation, procurement, and post-acquisition.

NIST SP 800-53 explains the security and privacy controls required of federal information systems and organizations. SP 800-53 is a catalogue of controls developed by NIST, and the defense and intelligence communities, deemed low, moderate and high impact. It also includes a lengthy list of 15 supply chain controls that spells out acquisition strategies, supplier reviews, trusted shipping and warehousing controls, the use of all-source intelligence, penetration testing and analysis of critical elements, as well as processes to address any known weaknesses.

NIST SP 800-161 specifically explains supply chain risk management for federal information systems and organizations. The goal via this document is to steer clear of products and services that may have been manipulated along the supply chain and now contain malicious functionality, counterfeit parts, or are exposed because of poor manufacturing or development practices. SP 800-161 not only explains the risks and threats posed to federal systems by the supply chain, but also explains how to integrate a supply chain risk management framework and controls into an agency's overall risk management operation using the Frame, Assess, Respond, and Monitor approach.

SUPPLY CHAIN CONCERNS MANIFEST THEMSELVES IN THE REAL WORLD

Probably the best public example of action taken by the federal government against a potential threat to its supply chain surfaced in 2017 when Russian security company Kaspersky Lab was banned for use and further procurement by federal agencies. In September 2017, the Department of Homeland Security mandated

that agencies audit federal systems for instances of Kaspersky software and discontinue its use.

The U.S. government perceived Kaspersky as a threat in the wake of Russia's alleged intervention via influence campaigns in the 2016 presidential election. Since Kaspersky's products monitor customers' systems for malware and other threats via servers based in Russia, the U.S. chafed at the Russian government's ability to compel Kaspersky to share customer data with intelligence operations in that country. Kaspersky issued strong denials that it has knowingly collaborated with the Russian government in such a manner, but the risk was too great for the U.S. government to absorb and it took the extreme and unprecedented measure of banning Kaspersky software from its systems.

The challenge, however, became immediate and apparent for U.S. agencies: Kaspersky has a massive presence not only on endpoints worldwide, but through partnerships with numerous third-party vendors, it's software could be embedded in any number of places. This is a strong illustration of the issue facing public-sector agencies when it comes to understanding the supply chain of its suppliers. Suddenly, a trusted U.S.-based network provider, for example, could have an established relationship with Kaspersky, throwing those products into question as well.

Geopolitics are playing a role in other sectors as well, and can be a deciding factor in determining what technology lands inside a federal agency. In August, for example, U.S. President Donald Trump signed a bill largely banning the use of Huawei and ZTE mobile technology by federal agencies and its contractors. The bill was part of the Defense Authorization Act. The Chinese telecommunications giants are viewed as a national security threat in some circles, though the bill allows for some components to be used provided they are not used to route or view data.

Meanwhile, a bipartisan bill introduced in June, meanwhile, called the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA), arrived in the wake of the Kaspersky and Huawei/ZTE rulings. While FASCSA awaits its day before lawmakers, many wonder about its impact on procurement policies and processes going forward, and whether it would address any perceived shortcoming in the NIST 800-series standards regarding supply chain risk management.

Senators Claire McCaskill and James Lankford introduced the bill which would establish a cross-agency council called the Federal Acquisition Security Council that would develop criteria and processes for assessing supply chain threats and vulnerabilities, sharing information among executive agencies, issuing guidance for incorporating risk information into procurement processes, and developing standards for supply chain risk management. The council, according to the bill, would act in the Executive branch of government and include members of NIST, OMB, General Services Administration, the intelligence community, and the Pentagon.

"Our bill creates a government-wide approach to solving supply chain security issues in federal acquisitions," Lankford said.

CONCLUSION

The public-sector supply chain and current procurement standards invite complexity and create a potentially vast attack surface that can be exploited. The confidentiality, integrity, and availability—the three tenets of information security—of federal IT systems is put at risk by exploitable vulnerabilities introduced at any point of the supply chain. This would include buying products or parts from unauthorized distributors, or failing to audit them for interdiction, or review them for patch levels and updates. Any comprehensive evaluation of vendors supplying the public sector should include a discussion and audit of each supplier, as well as intelligence related to known adversaries, threats and vulnerabilities to the supply chain.

The necessary guidance in the form of NIST recommendations—in particular NIST SP 800-161—exists to help agencies evaluate and frame risk in such a manner that the integrity of critical systems is preserved. Also, the introduction of the FASCSA bill aims to provide legislative protection from buying software and components from companies with known ties to unfriendly governments.

Supply chain risks to the public sector can pose consequences beyond an unreachable web server or a crashing laptop. The threat to data processed and stored by federal IT systems poses a threat to personal safety of government employees and to national security. It's an unacceptable risk to the federal government, and one that's being addressed by a mix of policy, process and technology.

This report was authored by Mike Mimoso with contributions from Aaron Shraberg. A special thanks to the entire Flashpoint team for supporting this report.