National Counterintelligence and Security Center
Supply Chain Directorate

Supply Chain Risk Management

Intelligence.Gov Background Paper

Introduction: this paper was developed to enhance public awareness of the Intelligence Community's Supply Chain mission, and is posted at the *intelligence.gov* website.

BACKGROUND:

The U.S. is under systemic assault by foreign intelligence entities (FIEs) who target the equipment, systems, and information used every day by government, business, and individual citizens. These threat actors capitalize on the culture of openness and collaboration in the United States to steal information to advance their military capabilities, modernize their economies, and weaken U.S. global influence. Adversaries have broadly targeted our intelligence, defense, and security communities, other U.S. Government agencies, academic and research institutions, and the private sector to misappropriate technologies and critical knowledge.

Our adversaries have augmented their traditional intelligence operations with nontraditional methods, including economic espionage, supply chain exploitation, and the use of students, scientists, and corporate employees to collect classified and unclassified information. Crucially, some threat actors are developing offensive capabilities that could be employed in a crisis or conflict to exploit, disrupt, and damage critical U.S. infrastructure. Supply chain exploitation, especially when executed as a blended operation in concert with cyber intrusions, malicious insiders, and economic espionage, threatens the integrity of key U.S. economic sectors, critical infrastructure, and research/development that the U.S. depends upon for security and economic growth. The scale of these hostile efforts are placing entire segments of our government and economy at risk.

A major factor enabling supply chain threats has been the globalization of our supply chains, characterized by a complex web of contracts and subcontracts for component parts, services, and manufacturing extending across the country and around the world. The multiple layers and networks of suppliers in this chain are frequently not well understood by either manufacturers or consumers. Our most capable adversaries can access this supply chain at multiple points, establishing advanced, persistent, and multifaceted subversion. Our adversaries are also able to use this complexity to obfuscate their efforts to penetrate sensitive research and development programs, steal intellectual property (IP) and personally identifiable information (PII), insert malware into critical components, and mask foreign ownership, control, and/or influence (FOCI) of key providers of components and services. Individually and in total, these supply chain attacks erode our nation's competitive advantages in commerce, technology, and security.

CURRENT STATUS:

Our adversaries are not bound by political borders or organizations, nor constrained by legal, diplomatic, or regulatory frameworks. A hostile foreign intelligence entity can hide its' presence by operating through multiple front organizations, companies, hackers, and organized crime, making it extremely difficult to discover and counter their actions. Identification and attribution of supply chain exploitation is further challenged by the clandestine nature of most attacks. For example, recent attacks have targeted key weapons programs (such as the Joint Strike Fighter compromise), sensitive information (such as the Office of Personnel Management data breach), and critical infrastructure (including the electric power and medical services sectors.) These attacks represent only the "tip of the spear". Novel means of attack, such as the expanding use of private companies as threat vectors, are only now beginning to be understood.

Even as the U.S. government and private sector have implemented programs to mitigate and counter supply chain threats, the evolution of directed, sophisticated and multifaceted threats threatens to outpace our countermeasures. Traditional remedies such as trade agreements, economic sanctions, and legal actions are reactionary in nature and cannot keep pace with the evolution of threats.

ODNI recognizes that countering and defeating supply chain threats necessitates two lines of effort. First, an evolving partnership between the government and private sector to develop means to *deter* and *disrupt* supply chain threats through advanced analysis, threat management, technology development, and information sharing. And, second, collaboration among acquisition, intelligence and security, and technology leaders in government and the private sector to establish a deeper understanding of adversary intentions and capabilities, and jointly develop capabilities to *detect* and *defend* against these threats. Our cooperation must extend across government and commercial "stovepipes" to account for interdependencies between critical sectors.

ACCOMPLISHMENTS:

The National Counterintelligence and Security Center (NCSC) is emphasizing the necessity to strengthen supply chain defense through broader awareness of threats and best practices to mitigate these threats. NCSC is raising national supply chain awareness through web based training, awareness videos, and best-practice documents for use by whole-of-government and the private sector.

To learn more about supply chain risk management and NCSC visit our website at *ncsc.gov and follow us on Twitter @NCSCgov*