2016
PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

Bulk Intrusion Data Analysis

Government and private sector networks that are core to the nation's critical infrastructure are subjected to an array of cyber penetrations, often targeting sensitive national and economic security systems and information. There is a need to identify best practices to organize and categorize – in a database – bulk intrusion data and to derive campaign analysis to understand cyber-attacks, with the potential to provide key public and private sector organizations the ability to prevent becoming a victim of such attacks. Education about the threat and mitigation measures are key components to begin addressing this pressing national security issue at the grassroots level. This team, following in the path set by last year's guide for individuals, has assembled a pamphlet for small to medium businesses to educate them on the implications of this revolution and to protect their livelihoods from cyberattack.

ISIL Finances

The Islamic State in Iraq and the Levant (ISIL) Finance Team evaluated ISIL's financial structure to determine how the Violent Extremist Organization (VEO) may generate and manage money across contested regions and controlled populations. The team identified and examined possible scenarios – Transnational Jihadi Brotherhood; Jihadi Territorial Authority; and Jihadi Caliphate – to determine how ISIL might change over the next three to five years. The three future scenarios considered internal and external environmental factors, and likely financial sign-posts that may indicate the VEO's shifting from one organizational structure to another. Additionally, the team examined ISIL revenue sources and expenditures, and the impact on each of the three scenarios. The team also provided a brief history, a background, and an overview of financial management and structure. The assessment aims to provide stakeholders with valuable insight while also encouraging discussion about ISIL's evolution and possible financial management strategies. The team did not endeavor to predict the future trajectory of ISIL nor definitively assert which financial resources would be needed to sustain each trajectory. ISIL's fortunes could rapidly change based on the focused attention given to the VEO.

Digital Blackmail as an Emerging Tactic

Digital Blackmail (DB) represents a severe and growing threat to individuals, small businesses, corporations and government entities. The rapid increase in the use of DB such as ransomware, the growth of variants and their ease of use and acquisition by cybercrime criminals, weak defenses, and the anonymity of the money trial will only increase the scale of attacks in the future. Private sector and government cybersecurity experts were brought together to determine emerging tactics and counter measures regarding the threat of DB. In this paper, DB is defined as the illicit acquisition or denial of access to sensitive data for the purpose of affecting victims' behavior. Threats of lost revenue, the release of intellectual property, or the destruction of critical data or reputational damage may be made. For clarity, this paper maps DB activities to traditional blackmail behaviors and explores methods and tools, exploits, protections, pay or not to pay, post attack actions and LE and government contact points. It also examines the future of the DB threat.

Impact on Supply Chain Security of Transnational Criminal Organization (TCO) Involvement in Non-Drug Crime

The primary focus of this report is to identify and illuminate the greatest risks from Transnational Criminal Organizations (TCOs) to legitimate supply chains, specifically in the Mexico and United States markets. Our findings show that supply chain security is a primary concern of the various private sector entities we contacted, despite the fact that their experiences in Mexico varied. With concerns ranging from whether to arm and escort trucks en route through Mexico, to increasing awareness of stolen cargo, companies face a wide breadth of challenges in securing their supply chains. Threats to the supply chain are not limited to a specific government agency and remain a persistent challenge. Communication and exchanges of information between the government and private sector are improving; however, further efforts at collaboration should consider that the objectives of the government and private sector do not always naturally overlap. Increased transparency among trusted partners would contribute to a common working knowledge from which further best practices can be gleaned.

Cyber Attribution Using Unclassified Data

Many of the country's leading retail, financial and governmental institutions recently experienced attacks and intrusions necessitating deeper understanding of cyber attributions of faceless attackers. Senior government officials, heads of agencies, corporate executives, investors, and others have a keen interest in findings in this area to support their decision making. The challenge of determining, deterring, and defending against such attacks – economically, politically, and militarily is driven by an accurate characterization and assessment of an anonymous perpetrator. Therefore, organizations must follow a structured approach to identify attacker data points. Organizations approach this problem in different ways, depending on their mission - law enforcement, intelligence community, or private industry. Models, such as the Diamond Model, may help, but they only provide a framework. Based on interviews and panel discussions with cybersecurity experts, this team's research addresses several Key Intelligence Questions related to Cyber Attributions. Focus areas include the relative importance of attributions to the Public and Private sectors, applicability of the Diamond Model, the state of methodologies and tools, and the identification of areas for further research.

Identifying and Mitigating Supply Chain Risks in the Energy Sector's Production and Distribution Networks

The traditional electric grid model of steady electric power produced from a coal, hydro or nuclear plant is changing rapidly from a one-way linear flow - from generation to consumption - into a two-way interactive network. Transmission and distribution operators take electricity produced from "just-in-time" pipelines (traditional power generators as well as renewables like solar and wind power) and communicate via smart meters and the Internet. This activity serves to monitor fluctuating generation in order to manage power flows to customers, who are also connected to smart meters and the Internet. This creates an interconnected system that is both highly efficient, yet potentially highly vulnerable. New equipment – including hardware, firmware, and software – is globally sourced and carries with it the potential for containing malware and hardware Trojans that can be activated by adversaries. The focus of this report is the supply chain risk of the electric grid including topical areas such as the energy supply chain risk management process and the roles and responsibilities of government and industry.

Leveraging the Internet of Things

The Internet of Things (IoT) is here and is transforming how we live and work. McKinsey Global Institute identified it as among the most disruptive technologies of the decade. Cisco estimates that the IoT will consist of 50 billion devices connected to the Internet by 2020 with an additional million devices coming online every month. This new landscape is global and manifests itself in everything from smart cities to agriculture to governance. The IoT identifies us, feeds us, transports us, informs us, and keeps us safe. Given these transformations, leaders in government must know what is on the horizon and start preparing for its impact. This study, which includes a White Paper and an accompanying infographic, is intended to help members of the IC better understand the potential implications of this changing landscape. Scoping this study was a significant challenge and our examination of IoT and intelligence is primarily intended to stimulate thinking and produce additional studies that explore these complex issues in more depth. Our approach was to look at IoT –enabled smart city environments focusing primarily on the IC's counterterrorism mission. The study describes some of the characteristics of the current and future IoT environments in Hong Kong and San Francisco and then addresses the collection issues within these environments where sensors will become ubiquitous and the volume of data for analysis will be immense, dispersed, and varied. A key element of this examination of IoT and intelligence is the unavoidable discussion of the implications for privacy and civil liberties.

Wireless Devices in the Workplace

U.S. Intelligence Community (USIC) analysts and subject matter experts from the Private Sector, co-authored this paper regarding the security and privacy of wireless devices in the workplace. This paper will describe how emerging wireless devices factor into the current wireless environment, and will identify wireless security and privacy issues with regard to the proliferation of wireless devices in the workplace. After addressing these security concerns, this paper will discuss and offer a proposed industry standard rating system for wireless devices so that consumers may easily understand the security risks posed by a particular device. As a model the team used the following Insurance Institute for Highway Safety (IIHS) ratings for passenger vehicles: Good, Acceptable, Marginal, and Poor. This observation led the team to propose a 5-Star rating system to reflect varying levels of security.

Applying Private Sector Media Strategies to Fight Terrorism

The ideological threat of violent extremism is a global problem with domestic implications. Extremist groups conduct continuous communications campaigns, targeting vulnerable and receptive individuals to get them to self-radicalize and conduct violence in the name of extremist ideologies. As evidenced by Americans who have joined terrorist organizations or conducted mass casualty attacks, such as those witnessed in Orlando, Florida, and San Bernardino, California, the implications of violent extremist propaganda campaigns are becoming more complex, more widespread, and more deadly. The Media Strategies Team conducted meetings with the private and public sectors to determine what strategies could be applied in US government-led efforts to counter extremist messaging. The results of this research outline the Countering Violent Extremism problem space, tools that the private sector uses for media strategy, and a framework for sustainable private sector engagement.