PREPARED STATEMENT OF

JOHN HULTQUIST, DIRECTOR OF INTELLIGENCE ANALYSIS, FIREEYE, INC.

BEFORE THE HOUSE HOMELAND SECURITY COMMITTEE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY

HEARING ON

SECURING U.S. SURFACE TRANSPORTATION FROM CYBER ATTACKS

FEBRUARY 26, 2019

Thank you, Chairman Richmond, Ranking Member Katko, Chairman Correa, and Ranking Member Lesko for convening this joint hearing today. We appreciate the opportunity to share FireEye's perspective on threats to the transportation and energy sectors and provide an overview of how the private sector is helping to secure those sectors.

Introduction

My name is John Hultquist, and I'm the Director of Intelligence Analysis for FireEye. My team of over 150 intelligence analysts and researchers pour over data we collect from FireEye's global networks of devices, managed defense of seven global Security Operations Centers, our incident response, researchers we have monitoring the criminal underground and many more sources to understand the global cyber threat. We have teams focused on criminal threats, cyber espionage, cyber physical, and strategic problems, as well as vulnerabilities. Ultimately, we provide intelligence reporting and services used by government and commercial clients around the world.

In addition to the 300-plus security professionals responding to computer intrusions, FireEye has over 200 cyber-threat analysts on staff in 18 countries, speaking 30 different languages, to help us predict threats and better understand the adversary – often by considering the political and cultural environment of the threat actors. We have an enormous catalog of threat intelligence, and it continues to grow everyday alongside the continually increasing attacks on organizations around the world.

FireEye is supporting the transportation and energy sectors here at home. We're protecting the Transportation Security Administration with both email and web inspection, managed by the Department of Homeland Security's Enterprise Security Operations Center. As TSA continues to stand up its intelligence capabilities, we are providing support through its subscription to our intelligence reporting.

Additionally, we assist in protecting the Department of Energy by supporting network and file inspection, malware analysis, and protecting their data from threats down to their endpoints.

We provide the ability for deep forensics inspection of all network traffic managed by the Department's Enterprise Security Operations Center. As DOE continues to enhance its cyber capabilities, we provide visibility to meet the Data Taxonomy Metrics. The Department is the largest civilian agency consumer of our intelligence reporting, which provides focused visibility into the threats targeted at the energy sector.

In addition to my role at FireEye I'm an adjunct professor at Georgetown University and the founder of CYBERWARCON, a conference on the cyberattack and information operations threat.

I have been working in cyber intelligence for over a decade, most of it at FireEye, but before that I worked as a contract cyber intelligence analyst with the Defense Intelligence Agency and State Department. Prior to that I worked briefly at the Surface Transportation and Public Transit Information Sharing and Analysis Center where I was an analyst exploring threats to the sector we will be discussing today. Part of my duties there were to forecast domestic threats by exploring global incidents. Though much of this work was focused on counterterrorism, I believe the methodology I employed there is applicable to this problem. If we want to forecast threats to surface transportation, we have to look globally for the actors who may target this sector, and explore not just how they carry out attacks, but why.

Today I will talk about a few incidents that have already affected surface transportation, but I will focus primarily on threats on the horizon that FireEye is watching develop in the Middle East, Ukraine, and South Korea, where Iran, Russia, and North Korea are most active. My team has had some success with this method. In 2014, we exposed an actor, who we call Sandworm Team, which was carrying out cyber espionage in Ukraine and who was soon after exposed in US critical infrastructure. A year later this actor caused the first known blackout by cyberattack in the Ukraine.

Pipelines

Criminal, state, and hacktivist actors have all demonstrated an interest in pipeline operators. Pipeline operators have been the victim of criminal ransomware incidents on multiple occasions. Hacktivist actors have threatened pipelines for environmental and other political reasons. We have seen some specific interest in pipeline infrastructure from state actors as well. APT1, an actor tied to China's People's Liberation Army, carried out an intrusion campaign attempting to gain access to pipeline operators in 2012. While we do not think the campaign aimed to cause any immediate effects, at the time we did assess that it was reconnaissance of our infrastructure that could be leveraged over the long term.

Despite the dearth of additional specific examples of pipeline targeting, targeting the sector is consistent with the behavior of several state actors who have carried out disruptive and destructive operations. Pipelines sit at the nexus of two well-established interests for these state attackers: energy and transportation. Despite a relatively brief history of disruptive and destructive cyberattacks against critical infrastructure, several incidents have focused on these sectors where the potential for cascading economic and psychological effects on the target population is considerable.

Energy, particularly oil and gas and the electrical power industry, has been the continued focus of threat actors who have either carried out disruptive cyberattacks or who appear to be tasked with preparing for such an operation. Destructive and disruptive attacks on oil and gas have almost become common in the Middle East where our U.S. adversaries are showcasing their capabilities and improving their skills.

For example, oil and gas has been the major focus of a long-term destructive campaign by Iran in the Gulf using destructive malware commonly referred to as “Shamoon.” Though these attacks have targeted critical infrastructure organizations, they have primarily affected business-focused IT systems rather than the sensitive control systems which run production. Nonetheless, Iranian sponsored threat actors caused significant, costly disruptions from 2012 to as recently as December 2018, the last time we observed one of these incidents.

The Middle East was also the scene of the most disconcerting attack on control systems we have observed. An industrial plant there suffered a disruption when attackers inadvertently triggered a shutdown using malware we call TRITON. They triggered that shutdown because they were attempting to manipulate automated safety systems, one of the last lines of defense to protect human life. We believe the attackers were developing the ability to create an unsafe condition using the control systems, while simultaneously disabling the safety systems designed to mitigate the attack. Such a scenario could have led to major disruption of operations, economic loss, and even loss of life. We believe this activity originated from a Russian government organization called the Central Scientific Research Institute of Chemistry and Mechanics. It is unknown whether these actors had been tasked to target the plant for some specific geopolitical goal or if they were using this Middle Eastern facility as a testbed to improve their capability.

In principal, methodologies honed in the Middle East against oil and gas could be applied to our pipeline sector. Destructive attacks could be used to interrupt the administration of these complex systems, potentially causing economic repercussions that cascade through the myriad of downstream users who depend on reliable service. A more complex scenario, like the TRITON incident, could also target pipelines, which could be manipulated to potentially disastrous consequences if actors can gain access to control and safety systems.

Transportation and logistics systems have been an underrecognized but fruitful focus for state cyber attackers as well. During and between well-known attacks in Ukraine which turned off the power to portions of the country, attempts were made by the same Russian actors to gain access to rail, air, and sea transportation routes and hubs, to varying degrees of success. In fact, we saw evidence indicating that while they were prepping the first attack that briefly disabled power service in the Ukraine, the actors we call Sandworm Team were also compromising airport and rail services. There are plausible but unverified reports of an attack which lead to disruption of rail service coincided with the second attack on Ukraine's grid.

As in the case of the Middle East, in Ukraine, we see technically complex cyber attacks that strike at the most sensitive industrial control systems, such as those that caused blackouts, as well as attacks that are not focused on these systems at all. Both types of attack have been successful. While grid attacks were undoubtedly watershed events, the most economically damaging attack we have ever encountered was fake ransomware called NotPetya. This fake ransomware encrypted drives just like its real criminal counterpart, but the state actors behind it never intended to decrypt this information for any amount of money, essentially making it a destructive tool. The malware spread rapidly, locking up vital systems and causing major disruptions to global companies. The result was over ten billion dollars in damages, according to one White House estimate. Most notably, however, many of the companies which posted major losses in the hundreds of millions were in the logistics business, despite this industry not having been specifically targeted. Such a pattern could indicate that logistics organizations may be especially economically vulnerable to cyberattacks of this nature.

Transit

Like pipeline operations, transit networks have been subjected to ransomware operations and denial of service attacks, which have, on occasion, resulted in disruption to service. Ransomware, which has affected many municipal services, has been used to hold transit systems hostage in return for payment. An attack like this in San Francisco took tickets systems offline, but operations continued when riders were offered free passage. In most cases we believe the attackers were financially motivated, though it is worth noting that these incidents expose a vulnerability that state actors, who have used a fake ransomware capability, could exploit.

In addition to ransomware incidents, the websites associated with mass transit systems, which are often crucial to their business, have been subjected to denial of service attacks. These incidents, which involve the use of a network of hijacked computers to jam a website with bogus traffic, have in some cases frozen operations. We have seen this phenomenon as far afield as Ukraine and Sweden. In 2017, transit systems in Sweden came under a prolonged attack by an unknown actor who disrupted travel. It is worth noting that like ransomware, denial of service is a capability used by state actors. And just as ransomware allows these actors to carry out attacks while hiding their true intentions, state actors have purported to be hacktivists and taken credit for denial of service attacks, hiding their hand it the operations. This was the case in the US, where Iranian hackers attacking our financial system claimed to be a pan-Arab hacktivist. Furthermore, there is a reduced barrier to entry for these types of attacks, and even states without this capability could source it from the criminal underground.

The complexity of transit networks and the potential for cascading economic consequences from disruption bare similarities to pipelines; however, transit networks offer an additional attraction to would-be attackers – transit is a highly visible sector with which the public regularly interacts. This factor is especially relevant as many cyberattacks appear to be more focused on psychological effects and undermining confidence in institutions than creating lasting physical effects.

One example of a highly visible cyberattack which affected the populace is the destructive campaign against South Korean media and banking in 2013. Though this campaign failed to interrupt broadcasts, it did interrupt some banking services, including online banking and ATMs. The result was a visible crisis that affected the everyday lives of South Koreans and which might have been even greater if broadcasts were halted. Blackouts fall into this same category of having far-reaching psychological effects. A disruption to transit could have a similar effect.

Conclusion

Thus far, U.S. critical infrastructure has been probed by actors from China, Russia, Iran, and North Korea. In many cases, these actors have focused heavily on electricity generation; however, our experience with them abroad suggests a much broader interest in creating disruptive or destructive effects. We should take these lessons to heart now and prepare for incidents across the transportation sector.

It's important to bear in mind that our adversaries are not necessarily preparing for a doomsday situation, or any lasting blow, but an asymmetric scenario where they can project power within our shores. Ultimately, their aim may be to sow chaos rather than achieve some complex military objective. Nonetheless, these incidents could have economic and psychological effects we cannot ignore.

Thank you again for the opportunity to participate in today's discussion. And thank you for your leadership improving cybersecurity in the transportation and energy sectors. I look forward to working with you to strengthen the partnership between the public and private sectors and to share best practices to thwart future cyber attacks.