DRAGOS

COUNTERING RANSOMWARE IN CRITICAL INFRASTRUCTURE

PREPARING FOR THIS CYBER THREAT AND THOSE THAT WE WILL UNCOVER

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS OF THE COMMITTEE ON ENERGY AND COMMERCE OF THE HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

20 JULY 2021, RAYBURN HOUSE OFFICE BUILDING

https://energycommerce.house.gov/committee-activity/hearings/hearing-on-stopping-digital-thieves-the-growing-threat-of-ransomware

Robert M. Lee[1]

I. Background

Chairman Pallone, Jr., Chairwoman DeGette, Ranking Members Rodgers and Griffith, and members of the committee, thank you for providing me the opportunity to testify before you today. It is an honor to be here before you to talk about cyber attacks in our critical infrastructure. My name is Robert M. Lee, and I am the CEO and co-founder of Dragos, a cybersecurity technology and services firm focused explicitly on the operations and industrial systems that our critical infrastructure depend on. I also currently serve on the Department of Energy's Electricity Advisory Committee as the Vice Chair of the Grid Resilience for National Security subcommittee and on the World Economic Forum's electricity and oil and gas cybersecurity subcommittees.

I started my career as an Air Force officer and spent most of that time tasked to the National Security Agency where I built and led a first-of-its-kind mission to hunt for, identify, and analyze state and non-state actors targeting industrial control systems. At that time, cyber threats towards industrial systems were seen as a possibility but not as a reality. The problem though is everyone was looking in the wrong location. Analysts around the community were hunting for threats in Enterprise information technology (IT) networks such as those that people depend on for email and personal computer usage. What we

[1] CEO and Co-Founder of Dragos, Inc.
@RobertMLee

were not doing is looking in the industrial and operations networks themselves. Broadly I will refer to this as operations technology (OT).

The easiest way to explain OT is to consider everything we have in IT networks plus physics. We have purpose-built control systems, different communications, and application programs you will not find in IT networks. But even if all the systems and networks converged the difference would fundamentally be the mission and its interaction with the physical world around us. When adversaries target IT networks they often steal data such as personnel records and emails and when they disrupt them with malicious software such as ransomware it impacts workers' ability to perform their job. When adversaries target OT networks they can steal data such as intellectual property as well, but they can, intentionally or not, also create unsafe conditions that cause damage in the world around us up to and including the loss of human life. The mission in OT is different. The threats to OT are different. Thus, the security and approach we take to those environments must also be different.

For decades, critical infrastructure companies have spent significant number of resources protecting their enterprise IT environments as they were asked to do. The belief was that OT networks were disconnected or highly segmented from other systems and that by protecting IT you would protect OT. As I mentioned though, we did not see the various OT threats that existed because the broader community was looking for OT threats, in IT networks. We lacked the visibility in OT to determine what was going on. In essence we had the equivalence of Schrödinger's OT believing that as long as we did not look in the box the cat was alive.

In my time at the NSA, we started looking in the box. To our surprise, we found a wide variety of state actors, beyond even the normal ones we refer to, targeting and performing reconnaissance against these systems. Leading critical infrastructure companies that were communicated to by various government agencies sharing our findings began to increase their defenses as good stewards of public interest and national security. Unfortunately, many of the efforts were essentially copy/pasted IT security approaches and standards into OT. Many of these approaches predictably failed or under delivered. That is what led me to leave the US government and found Dragos so that we could take an OT specific approach to our cybersecurity software and services.

Since the founding of Dragos the threat landscape has become far more illuminated though we are still in the early days of fully scoping the problem. In 2015 the first ever cyber attack to cause an electric power outage took place in Ukraine and I was privileged to lead up a portion of that investigation with other wonderful individuals to include Michael Assante, Tim Conway, and Tim Roxey. In 2016 the second ever cyber attack to cause a power outage took place again in Ukraine and my firm was involved in analyzing the malicious software leveraged. In 2017 my team was again involved in analyzing malicious software at the center of a major attack, this time it was against a Saudi Arabian petrochemical company, and it was the first time ever that a cyber attack explicitly targeted human life. The adversary made a mistake, otherwise dozens of people would likely have lost their lives. Over the next few years my team tracked those same threats and others as they carried out operations in other countries across the Middle East, Australia, New Zealand, Europe, and numerous operations in the United States. Today we track over 15 different state actors that explicitly target industrial and operations systems across numerous critical infrastructure industries. We have also begun to seen OT specific ransomware.

In the last year things have continued to accelerate. The SolarWinds supply chain compromise that gained a significant amount of attention in IT networks was also widely leveraged in OT. While this fact remained unreported, Dragos responded to numerous incident response cases in OT where companies significantly lacked the visibility and data collection to determine if they were compromised or not. While the espionage that took place in SolarWinds made people uncomfortable, what should have scared people is the fact that a hostile foreign adversary had direct access, whether or not they knew it, to sensitive critical infrastructure sites across the US and that broadly we were unprepared to identify if the adversary was even still present. We are fortunate it was an espionage operation and not a destructive one.

Again, in a concerning development, an adversary targeted a water facility in Oldsmar, Florida. While the technical details of the case are not all that interesting or advanced the underrepresented point is that a foreign actor attempted to poison American citizens' water. Targeting human life should always be off limits and unacceptable. The fact that adversaries are already trying continues to cross any of our imagined red lines as they become bolder and more capable. Unfortunately, my assessment is we will have a loss of human life scenario as a direct result of cyber operations against OT in the future. I do not know when, and what we must work together on is ensuring that when it occurs it is as limited as possible understanding that no loss of life scenario is acceptable.

Specific to the topic of ransomware, my firm has responded to numerous ransomware incidents in OT that have gone unreported. Each company has done the right thing to get help and remediate the issues at their own cost. However, these incidents happen far more often than people realize. These cases tend not to make the news because the disruption does not rise to a level that is noticeable especially when companies have resiliency in their industrial operations and what they produce. Across all the cases though we continue to see that a lack of visibility in the OT networks leads companies to believing they are in a better place than they are and when the incident occurs, they do not have the appropriate plans or investments made to prevent breaches, detect threats, and when necessary, respond and recover efficiently. These companies are often resource strained. There is not a need for a moonshot project, no buzzwords like AI or blockchain are necessary, instead these companies need to understand the problem better and they require resources to adopt commercial technologies and services already available while increasing and resourcing their security staff appropriately.

Our hearing today appropriately is on ransomware as it is far reaching, accelerating, and impactful to daily life in this country especially for its disruptive qualities in critical infrastructure. But I want to underscore that it is just one risk facing our infrastructure and if anything highlights that if criminals can be successful in breaching and disrupting our OT environments, state actors will find much more success.

However, there are successes we can and should point to and emulate. The threats are worse than we realize, but not as bad as we want to imagine. And ultimately defense is doable.

To do this today I want to highlight five key points all inside of a theme of harmonizing roles and responsibilities between private sector and government. I think this can help us address ransomware in OT and set us up for success and derivative effects against state actors.

II. The Five Key Points

1. To defend against ransomware, we must first find a way to harmonize the roles and responsibilities of the private sector with government and the government's need to be aware

of critical breaches. There are significant and important roles and responsibilities that government has but there are also significant expertise and capability that the private sector can bring. Sometimes this can be confusing in messaging to the private sector on what the government can and should be doing in any given case. As an example, when a breach happens that is made public, companies often get asked why they did not bring in government agencies for incident response. But if those companies have already engaged reputable private sector incident response teams that should not matter. The government should be made aware of any incidents that can impact national security or critical infrastructure's ability to deliver their goods and services but do not need to be an on the ground team responding to incidents. Candidly, those teams are amazing people and ready to help but have less expertise and experience on the topic than the top end incident response firms that specialize in those cases. It is good for the private sector to be able to leverage government resources but the most important mission for government cybersecurity teams is protecting government networks and systems and then sharing what they have learned while amplifying the risks they see to educate others.

2. There must be a simplified unburdened process and single point of contact with the government. Whichever government agency is on lead does not matter as much to the private sector though it seems the right answer is CISA. The important thing is that there is only one front door to the government who can then coordinate the interagency and communicate clearly to the private sector entity. Right now a typical power company CEO as an example can expect to hear from the DOE, DHS, National Guard, FBI, DOD base commanders in their service territory, and others on when and why they should contact that government agency, often with conflicting guidance, and their focus areas which amount to a differing set of goals across government. A front door to government communicating the government's strategy, requirements, and assistance would greatly reduce the confusion that can occur.

3. Ransomware in OT is exposing the underinvestment in cybersecurity in many organizations. My prediction is as we counter this threat together the community will gain much more insight into the state intelligence and military units' activity in this space. We must be prepared for what we find and think about the ransomware strategy as part of the overall cybersecurity strategy. Ransomware cannot simply be the flavor of the day but instead a rallying effort of the community to increase cybersecurity overall.

4. Critical infrastructure companies stand ready to do the right thing and partner with government fully. However, differing regulation regimes and requirements can distract from the focus. Whatever regulations manifest they should be thought of together so that companies do not have overly burdensome requirements on them as we all try to achieve the same goal of security. As an example, some power companies have natural gas operations as it is a significant fuel source in our electric system. A power company may already comply with NERC CIP cybersecurity regulations. Many of those companies have extended their security practices proactively into non-NERC CIP covered assets including distribution substations and gas pipelines just trying to do the right thing. Yet new requirements such as TSA's pipeline regulations do not consider this and at times are in conflict with already existing regulations and

cybersecurity standards or not appropriately tailored to OT. This puts those power companies and others in a position where they have rip and replace their already existing security standards that have worked for them with new guidance they are unfamiliar with in practice. This can have a net negative security impact on an already strained security workforce at these companies. Policy actions around regulation should look to drive outcomes such as the reliability of critical services instead of being prescriptive and ignoring existing efforts.

5. Government should communicate the *why* and the *what* to private sector but leave the *how* to the individual entities. We have seen this work very well. This Administration and the Department of Energy launched a 100-day action plan earlier this year focused on OT cybersecurity in the electric sector. The goal was increasing real time information sharing, visibility, detection, and response capabilities in OT. The government laid out the requirements and why this was important. It was not a laundry of list of asks but instead a straightforward assessment of the problem and a few direct asks to the private sector. This was done in concert with the private sector leveraging the Electric Sector Coordinating Council which is a CEO led group across the electric system. The government asked for the effort to be done but did not dictate how it would be done. The electric sector coordinated, evaluated what was on the market, and chose Neighborhood Keeper, a technology made by Dragos in cooperation with the Department of Energy. They then deployed it quickly, voluntarily, and at their own cost. This was a monumental undertaking that has never been achievable before in OT and was a success because the private sector knew what mattered to the government and the requirements to hit but were left to innovate on how they achieved success in ways that worked for them. As a result, we went from less than 5% of visibility across the electric community to more than 70% of the electric system in the US today being monitored with information sharing across each participant in real time as a collective defense. That information is shared with the Electricity Information Sharing and Analysis Center (E-ISAC). Other industries have paid attention to the electric sector's leadership and the White House's efforts and there are now many in the water and gas sectors that are already adopting the same technology and approach to help national security. As an example, the Downstream Natural Gas ISAC (DNG-ISAC) has signed on to do the same work that the E-ISAC is doing across their community. All of this is done while protecting the data and identity of the participants. The system is entirely anonymous and all the data stays in the company's networks. This allowed the entities to be comfortable sharing insights with the government including ongoing threats, vulnerabilities, and compromises while protecting themselves and sensitive data. Government setting requirements and amplifying those requirements is important. Letting the private sector figure out how to achieve those requirements in ways that work for them and leverage their expertise running our infrastructure is paramount.

I sincerely thank the Committee for providing me the opportunity to testify today and welcome any questions or additional information.