CISA Summit Day one

The Cybersecurity & Infrastructure Security Agency (CISA) began its 3rd annual cybersecurity summit yesterday. Day one was devoted to general cyber insights from several key perspectives that included the FBI, Department of Homeland Security, CISA, and The Secret Service among others. As self-described, CISA is the nation's risk advisor whose mission is to serve both public and private institutions with the most comprehensive and up to date risk assessments regarding all things cyber-related. As the Director of CISA Christopher Krebs said, "we are the calvary".

Overseeing 3 million endpoints and digesting an estimated 7.2 terabytes of data daily, CISA is charged with being the point man in securing the country's digital transformation, whose agency motto is "defend today and secure tomorrow". Some of their insights gleaned from our current Covid 19 experience is that threat actors have increased the activity designed to create fear, uncertainty, and doubt. That phishing is still the #1 attack that sets the hook for APT across all platforms. That misinformation campaigns from nation-states like China and Russia have greatly increased activity with 7,000 new fake domains identified and removed in 2020 alone to date. Also, typo-squatting and water-hole attacks are extremely prolific as well.

The first panel of the day addressed Ransomware with representatives from CISA, FBI, DHS, and the Secret Service participating. The FBI reports that in 2013 it would have been one computer that was attacked for only $100's ransom, then by 2015 entire networks were targeted seeking $10,000's of thousands, and that by 2019-2020 it is common to see $100,000's and sometimes Millions in ransom demands. Attackers are getting more sophisticated in techniques for holding data captive adding threats to leak data to the public if ransom not paid. The FBI is aware that cartels have formed that now share data and share resources like malware authors, money mules, and operations systems.

RAaS (ransomware as a service) is becoming very popular now allowing cartels to increase their attack surface and speed to market. They have RAaS based subscriptions that have grown, according to the FBI, into an entire ecosystem including customer service that supports Ransomware activities. Furthermore, all the agencies agree that investigating the RW attacks is very difficult and takes time, especially because the bad guys all use the anonymous TOR network to communicate and take only Bitcoin as payment which is very hard to trace. Also, the hackers are using email systems in various parts of the world that do not collect data on the user therefore having no information to share with investigators.

Since today cooperation between agencies is more fluid and productive by comparison to pre 9-11 days, the agencies agree that if you are a victim of Ransomware that you should contact whichever agency is in close proximity to your business to begin the investigation and that agency will coordinate with the other need to know agency groups to assist in the investigation. They repeated several times the importance of speed in getting involved as soon as possible in order to capture the important data which will assist them in prosecuting the perpetrators. The FBI did comment that they have been sometimes successful in capturing cash assets from the

perpetrators that sometimes are returned to a victim to help in compensation towards the overall cost of the insult.

All the agency representatives spoke very highly of the NCIJTF (National Cyber Investigative Joint Task Force) formed in 2008 which acts as an infosec clearinghouse of inter-agency critical data exchange. NCIJTF is comprised of over 30 partnering agencies from across law enforcement, the intelligence community, and the Department of Defense. Representatives are co-located and work jointly to accomplish the organization’s mission from a whole-of-government perspective. The agency's mission is to synchronize efforts aimed at identifying, pursuing, and defeating terrorists, spies, and criminals who seek to exploit our nation's cyber systems.

The overarching theme from Day one was to punctuate the fact that we are stronger when we work together than when we all "play a giant game of whack-a-mole fighting this never-ending battle" said Assistant Director Wray of the FBI in the closing comments of the day. He referenced how quickly the FBI and the other national enforcement agencies were able to pivot after 9-11 "changing from 1st gear to 5th gear on the fly" to show how the FBI is now taking leadership to adapt our nation's cyber response capabilities from street-level to an enterprise-level response. Explaining how the FBI is working with NCIJTF leading the partnership of both public and private entities to build a team approach to cybersecurity fostering an atmosphere of trust and cooperation. It was, in the end, very encouraging to know that the nation's law enforcement eyes are now fully focused on the problem of cybersecurity seeking solutions.