THE UNITED STATES DEPARTMENT of JUSTICE

Deputy Attorney General Lisa O. Monaco Delivers Keynote Address at International Conference on Cyber Security (ICCS) 2022

New York, NY

~

Tuesday, July 19, 2022

Remarks as Prepared for Delivery

Thanks so much, Ed. It's great to be back at Fordham and ICCS. It's also great to be sharing the stage with another former federal prosecutor – President Tetlow. I see great colleagues and friends in the audience from my previous tours at the White House and the government. It's also great to be here in person for the first time since COVID began.

The FBI and Fordham University convene this forum for experts and leaders to discuss the complex cybersecurity challenges facing our country. And every year, those challenges get more and more pressing.

The last time I spoke here, I sat in a different seat in government; I was President Obama's Homeland Security and Counterterrorism Advisor. I was part of the team that briefed him every morning on the urgent threats facing our nation. And over those years, I spent more and more time during that morning briefing him on cyber threats – in particular, nation-state actors.

Since returning to the government and in my current seat as the Deputy Attorney General, I have been struck by an evolution: malicious cyber actors becoming more aggressive, more sophisticated, more belligerent and brazen – and an increased blurring of the line between state-sponsored cyberattacks and attacks by criminal groups.

At the Justice Department, keeping the American people safe from all threats, foreign and domestic, is an essential part of our mission. That is why, over the last year, we have been focusing on attacking cyber threats from every angle. We are taking a proactive approach to the threat. That approach has been informed by a Comprehensive Cyber Review conducted over the last year – the final report of which we are releasing today.

Building on the work of cyber experts in the Justice Department from across Administrations, our focus has been on increasing our capacity to disrupt and to respond to malicious cyber activity. And the report we release today reflects what we have learned over the last year, including the need to prioritize prevention, to ensure we are doing all we can to help victims, and above all else – to use all the tools at our disposal, working with partners here and around the globe, across the government and across the private sector. This approach has yielded real results. In the last year, those results – reflected in actions and disruptions – many of which began with critical reporting from and cooperation with companies who have been victims of cyber-attacks.

Today, I'm pleased to announce that this approach has produced real results again – thanks to rapid reporting and cooperation from a victim, the FBI and Justice Department prosecutors have disrupted the activities of a North Korean state-sponsored group deploying ransomware known as "Maui." That ransomware targeted U.S. medical facilities and other public health sector organizations.

Last year, a medical center in Kansas experienced the dread that faces too many critical infrastructure operators. North Korean state-sponsored cyber actors encrypted the hospital's servers – servers being used to store critical data and to operate key equipment. The attackers left behind a note demanding ransom, and they threatened to double it within 48 hours. In that moment, the hospital's leadership

faced an impossible choice – give in to the ransom demand or cripple the ability of doctors and nurses to provide critical care.

Left with no real choice, the hospital's leadership paid the ransom. But they also notified the FBI, which was the right thing to do for themselves and for future victims.

The FBI and Justice Department prosecutors immediately got to work on what was then a never-before-seen ransomware variant. They traced the ransom payment through the blockchain – just as we did in the aftermath of the attack on the Colonial Pipeline. Following the crypto-breadcrumbs, the FBI identified China-based money launderers – the type who regularly assist North Koreans in "cashing out" ransom payments into fiat currency. Additional blockchain analysis revealed that these same accounts contained other ransom payments. The FBI traced those to another medical provider in Colorado and potential overseas victims.

Now, all this digital sleuthing paid off several weeks ago: from the money laundering accounts, we seized approximately half a million dollars in ransom payments and cryptocurrency used to launder those payments. This recovery includes all the ransom paid by the Kansas medical center, plus what we believe are ransoms paid by other victims, including that medical provider in Colorado. And as a result of all this work, the FBI, and their partners at CISA and Treasury, shared the fruits of their investigation in a joint Cybersecurity Advisory regarding the Maui threat.

And today, we have made public the seizure of those ransom payments, and we are returning the stolen funds to the victims.

In sum, a medical center in Kansas did the right thing at a moment of crisis and called the FBI. What flowed from that virtuous decision was: the recovery of their ransom payment; the recovery of ransoms paid by previously unknown victims; the identification of a previously unidentified ransomware strain; all from an investigation that allowed the FBI and its partners to release a cybersecurity advisory to empower network defenders everywhere.

This approach attacks malicious cyber activity from every angle. It incorporates lessons from our fight against other national security threats like terrorism; it puts prevention first; it takes a victim-centered approach; and it uses all the tools at our disposal; and focuses on the reporting we receive from private sector companies, to maximize our ability to take down bad actors – and importantly to prevent the next victim.

This example and others over the last year show that we can and should borrow the tools we use in other spaces. And that is exactly what we are doing – the department is applying its successful approaches to the threats of the past to the cyber threats of today. Like our approach to terrorism, we must be intelligence-led, threat-driven and laser-focused on preventing the next victim of malicious cyber activity.

And that's exactly what we did earlier this year when the FBI and Justice Department prosecutors – working with partners internationally and here at home – disrupted a global botnet known as Cyclops Blink – which was under the control of the GRU, Russia's military intelligence agency. Now, importantly, we detected this botnet of victim devices and disabled the GRU's control over those devices before they could be used to initiate an attack – an attack against Ukraine, against us, against our allies. By working closely with WatchGuard, the manufacturer of the network devices targeted by the malware, and drawing on our in-house cyber talent to create the code and other technical solutions to identify and delete the malware, we were able to prevent that next cyber-attack. I want to acknowledge our cyber experts from Ukraine, who are with us today, who we are working with to combat Russia's unprovoked aggression against Ukraine.

Efforts like this are prime examples of public-private partnerships at their most effective and what the future of cyber looks like. It is not enough to engage in after-the-fact prosecutions of hackers – that's a lot for a federal prosecutor to say – but an increasing number of whom are working from safe havens abroad. With help from our partners, we can disrupt and dismantle the networks and capabilities before cybercriminals and state-sponsored hackers compromise their next victim.

But the reality is – as every single person in this room knows – we live in a world where it is impossible to disrupt all malicious cyber activity.

So we are also doing all we can to leverage our investigations to mitigate the harm to innocent victims, often with the help of the private sector.

The FBI took that approach last year when it obtained the decryptor key from actors who conducted the attack on Kaseya, threatening hundreds of downstream victims. Thanks to cooperation across the government and the private sector, the FBI was able to share the decryptor key with Kaseya and private sector partners, enabling the mass decryption of victim networks. Ultimately, we also charged R-Evil actors, one of whom was extradited to the U.S. earlier this year and will face trial in the Northern District of Texas. That's thanks to cooperation from, among others, Bitdefender, McAfee and Microsoft, the FBI and its partners were able to assist many of the victims of R-Evil's attack and to mitigate the harm to them and their businesses.

And none of this – none of this – would have been possible without Kaseya, which in their darkest hour made the right choice – again, they decided to work with the FBI.

Identifying and warning about the Maui variant and the Kaseya case exemplify the "all tools" approach to disrupting cyber threats.

Now, when we say "all tools," we mean using all the tools we have at our disposal – our law enforcement and criminal justice tools, our financial enforcement tools like sanctions and export controls, and tools used by our international and private sector partners. And over the past year we are increasingly using our law enforcement tools in new and innovative ways.

Case in point: last year, we used our criminal and civil forfeiture authorities to turn the tables on ransomware attackers and to follow the money and seize back a significant portion of the proceeds from ransom paid to DarkSide, the group that attacked the Colonial Pipeline, disrupting fuel transport on the east coast last summer. And in Cyclops Blink, the global botnet I mentioned earlier under the GRU's control, we used a tried-and-true law enforcement authority – a search warrant, that's right, a search warrant – to disrupt the botnet operation.

And the department's Civil Cyber-Fraud Initiative, which we launched last year, has applied our traditional expertise in civil fraud enforcement to hold accountable those companies that contract with the federal government and receive federal funds, but fail to follow required cybersecurity standards.

This initiative's work recently resulted in a defense contractor agreeing to pay $9 million to resolve allegations that it misrepresented its compliance with cybersecurity requirements in NASA and Department of Defense contracts – this is the second such settlement under this initiative. Holding contractors accountable for their cybersecurity promises will enhance resiliency against cyber intrusions across the government, the public sector and key industries.

"All tools" also means using everything at our disposal to target the ecosystem that fuels malicious cyber activities.

Focusing on the entire threat ecosystem is how we have long tackled national security threats – like, terrorism – and we've got to apply that approach to cyber.

This was our vision when we launched the Ransomware and Digital Extortion Task Force and the National Cryptocurrency Enforcement Team to develop new ways to address the explosion of ransomware and the abuse and illicit use of cryptocurrency.

Each of these actions underscore our clear message to cyber criminals and to nation states: if you target the American people, if you target our small businesses, our hospitals, our critical infrastructure – the Justice Department will target you.

But we know that our approach to these threats can't be done in isolation – our partners are critically important to all of this work.

We could not have carried out the Cyclops Blink botnet operation without the assistance of WatchGuard. Colonial Pipeline stepped up and reported quickly to the FBI that its computer network

had been accessed and that it had paid a ransom demand. And, of course, the Kansas medical center that I spoke about at the outset did the right thing by reporting their ransomware attack.

The key to our ability to take disruptive action is to work together. One of the most important steps in disrupting malicious cyber activity is to increase the reporting of cybercrimes by private sector victims or online platforms as soon as those crimes occur.

A significant accomplishment in this regard was the Cyber Incident Reporting for Critical Infrastructure Act of 2022 – a much-needed step towards ensuring that critical private sector entities report cyber incidents and ransomware payments to the government.

In implementing this landmark law, we will work with our partners at CISA and across the federal government to ensure that, as the reporting flows in, federal law enforcement receives the information they need and can rapidly use to go after the adversary behind the attack – and prevent the next victim. I applaud CISA Director Jen Easterly for her great partnership and commitment to ensuring that cyber incident reporting received by CISA is immediately shared with the FBI so it can used to claw back that ransom payment and disrupt that botnet.

Cooperation will allow us to follow the money, to extract decryptor keys and to prevent the next victim.

As the operations I've discussed today have shown, the information provided by the private sector is crucial to our disruption efforts, and allows the department to identify the evidence, victims and infrastructure associated with these crimes.

As the private sector faces cyber threats, inevitable questions will arise: Why should we go to law enforcement? Where are the benefits? What's in it for me and my company?

The answer is that if you report that attack, if you report the ransom demand and payment, if you work with the FBI, we can take action; we can follow the money and get it back; we can help prevent the next attack, the next victim; and we can hold cybercriminals accountable. Those companies that work with us will see that we stand with them in the aftermath of an incident.

The bottom line is this: we are all in this together. It is bad for companies and bad for America if we don't work together on these issues.

But we need our partners in the private sector for more than reporting and visibility into cyber attacks. We also need your know-how and your talent to prepare for the threats of tomorrow.

The department's cyber workforce is defending this country every day and I think it is punching well above its weight. The techniques used in the Cyclops Blink operation to identify the vulnerability in the botnet's command-and-control mechanisms, to impersonate the GRU's communications to that botnet, and ultimately to remove the malware, were developed with the in-house technical expertise of the department's FBI agents and prosecutors.

To do all that, and to increase the tempo of our disruption operations, we need to recruit more and retain more of the best class, cyber-savvy workforce at all levels. We need to build the next generation of prosecutors, agents, computer and data scientists and network defenders.

Yesterday, I visited the National Cyber-Forensics Training Alliance – a public-private partnership focused on increasing information sharing to identify, mitigate and disrupt cyber threats.

I was there to recruit the next generation for this work – to speak to students, recent graduates, professors, and career advisors from law schools and universities around New York.

I told them that the department, including the FBI, has a one-of-a-kind cyber mission that frankly you can't find anywhere else. It is a mission that allows even those fresh out of school, to identify cybercriminals on victim networks, in grey space and even on the hacker's own networks. Not only do our teams enforce the rule of law and neutralize bad actors, they take back ill-gotten gains, they cut off hacking infrastructure and convict hackers of crimes, all with the mission of protecting the American people.

I asked the students I met to be part of our next class of Cyber Fellows, a program developed out of our Cyber Review that I announced today. This is the group that will train the next generation of attorneys to tackle evolving cyber threats.

This fall, our first class of Cyber Fellows will join the ranks of the Justice Department and work on investigations ranging from state-sponsored cyber threats to transnational criminal groups.

So, I will take this opportunity – here at a great university – to repeat the message I delivered yesterday: we need the next generation's help. Join our ranks. I encourage the young talent in this audience to consider applying for future fellowship classes, or to consider other pathways to the department's. You are exactly what we need to address the cyber threats of today and tomorrow.

At the Justice Department, we will continue to work aggressively and relentlessly to keep our country safe from all threats, both online and off, and we need your help.

For those of you in the private sector, we need your reporting. For those students and young professionals out there, we need your talents. And for the many U.S. and foreign government personnel in the audience and elsewhere, we need your continued excellent work and partnership and commitment to the cause. Thank you for the work you are doing every day to keep our communities safe and to protect all that we hold dear.