

Remarks by Deputy Secretary of the Treasury Wally Adeyemo at the International Counter Ransomware Initiative Summit

November 1, 2022

WASHINGTON – Today, as part of the second International Counter Ransomware Initiative Summit, Deputy Secretary of the Treasury Wally Adeyemo hosted participants from 36 countries at Treasury to discuss the whole-of-government approach to the ransomware threat.

Treasury's Financial Crimes Enforcement Network (FinCEN) also released its Financial Trend Analysis of ransomware trends in Bank Secrecy Act (BSA) reporting data, showing a significant increase in ransomware filings during the second half of 2021. Ransomware-related BSA filings in 2021 approached \$1.2 billion, and roughly 75 percent of incidents reported to FinCEN during the second half of the year pertained to Russia-related ransomware variants.

[The FinCEN report is available here.](#)

Remarks As Prepared for Delivery

Thank you for the introduction, Anne, and thank you all for joining us.

It is a clear testament to both the grave threat that ransomware poses and the critical importance of international cooperation that we have such strong participation from countries across the globe during this Summit.

And not only do we have participants from different parts of the world, but also different parts of governments. I know that some of you lead or sit in your country's homeland security offices and intelligence agencies, while others come from departments of defense, ministries of justice, and law enforcement bodies, among others.

We may approach the challenge of ransomware with a different lens—and in some cases, an entirely different set of tools—but we are all here because we know that ransomware remains a critical threat to victims across the globe and continues to be profitable for bad actors.

In fact, we know that hackers around the world consider conducting ransomware attacks the most profitable scheme on the internet. More profitable even than selling illegal drugs via darknet markets and stealing and selling stolen credit cards.



In the midst of this landscape, it is more important than ever that we come together to share what we are seeing through our unique lenses and learn from each other's best practices.

Today, you are going to hear from my colleagues who represent the two main counter-ransomware arms of the Treasury Department: our Office of Terrorism and Financial Intelligence and our Office of Cybersecurity and Critical Infrastructure Protection.

And what I hope you see from their presentations is that while the work they each lead is important separately, we have found that when we work together in close coordination we can best amplify and reinforce our efforts. Not only is this true within Treasury, but across the entire government. In the United States, we are working together with officials that may employ different lenses to take a whole-of-government approach to respond to the serious threat of ransomware. I encourage you to do the same, from building connectivity within your own institutions, to unifying and supporting efforts across your governments, and finally by collaborating internationally through summits like this.

With that, I will hand it over to my colleagues to talk about Treasury's efforts in more detail.

Thank you.

###

