

ONE HUNDRED SEVENTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

August 30, 2021

Mr. Robert M. Lee
Chief Executive Officer
Dragos
1745 Dorsey Road
Suite R
Hanover, MD 21076

Dear Mr. Lee:

Thank you for appearing before the Subcommittee on Oversight and Investigations on Wednesday, July 20, 2021, at the hearing entitled “Stopping Digital Thieves: The Growing Threat of Ransomware.” I appreciate the time and effort you gave as a witness before the Committee on Energy and Commerce.

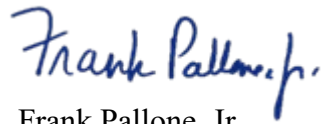
Pursuant to Rule 3 of the Committee on Energy and Commerce, members are permitted to submit additional questions to the witnesses for their responses, which will be included in the hearing record. Attached are questions directed to you from certain members of the Committee. In preparing your answers to these questions, please address your response to the member who has submitted the questions in the space provided.

To facilitate the printing of the hearing record, please submit your responses to these questions no later than the close of business on Monday, September 13, 2021. As previously noted, this transmittal letter and your responses will all be included in the hearing record. Your written responses should be transmitted by e-mail in the Word document provided to Austin Flack, Policy Analyst, at austin.flack@mail.house.gov. To help in maintaining the proper format for hearing records, please use the document provided to complete your responses.

Mr. Robert M. Lee
Page 2

Thank you for your prompt attention to this request. If you need additional information or have other questions, please contact Austin Flack with the Committee staff at (202) 225-2927.

Sincerely,

A handwritten signature in blue ink that reads "Frank Pallone, Jr." in a cursive style.

Frank Pallone, Jr.
Chairman

Attachment

Mr. Robert M. Lee

Page 3

cc: The Honorable Cathy McMorris Rodgers
Ranking Member
Committee on Energy and Commerce

The Honorable Diana DeGette
Chair
Subcommittee on Oversight and Investigations

The Honorable H. Morgan Griffith
Ranking Member
Subcommittee on Oversight and Investigations

Attachment—Additional Questions for the Record

**Subcommittee on Oversight and Investigations
Hearing on
“Stopping Digital Thieves: The Growing Threat of Ransomware”
July 20, 2021**

Mr. Robert M. Lee, Chief Executive Officer, Dragos

The Honorable Frank Pallone, Jr. (D-NJ)

1. The Department of Homeland Security, FBI, and other law enforcement assist with incident response, but I would like to understand whether we are providing victims the variety of resources needed beyond traditional law enforcement, such as technical expertise, recovery strategies, best practices on how to deal with the malicious actors, and other resources that may be required in order to ensure continuity of operations.
 - a. What more do you think the U.S. government can and should be providing to victims of ransomware attacks?
 - b. Do you have any recommendations for actions Congress may take in order to assist in those efforts?

The Honorable Diana DeGette (D-CO)

1. I am encouraged by the actions the Biden Administration has taken thus far, including the announcement of forthcoming cybersecurity performance goals for critical infrastructure and the formalization of the Industrial Control System Cybersecurity Initiative. Given the critical role the private sector plays in both the operation and security of our critical infrastructure, I would like to hear your take on its response to these threats and to the initiatives and requirements being announced by DHS and other agencies. How do you rate private industry’s response thus far and is there anything Congress can be doing to further incentivize the private sector to take these threats seriously?

The Honorable H. Morgan Griffith (R-VA)

1. Recently, a ransomware attack occurred during the Fourth of July holiday weekend on the Florida information technology company Kaseya. President Biden commented on the impact of the ransomware attack that it inflicted only “minimal damage to U.S.

business, but we're still gathering information.”¹

- a. To date, what information is known about the damage caused by this attack?
- b. What type of damage is expected to result from ransomware attacks?
- c. Kaseya stated that the attack never affected critical infrastructure. How does Kaseya define “critical infrastructure?” Does its definition include transportation networks, electrical power grids, health care facilities, governmental entities, etc.?

The Honorable Michael C. Burgess, M.D. (R-TX)

1. In May, a ransomware attack shut down the Colonial Pipeline company's operations for nearly a week. This act cut nearly half of the southeastern United States' transportation fuels.
 - a. How can we make our critical infrastructure more resilient against ransomware attacks?
 - b. Is it possible to compartmentalize critical infrastructure so that attacks have smaller impacts?
 - c. Should infrastructure have physical fail-safes to ensure continued operations during a cyber-attack?
 - d. What can individuals do to better protect themselves and their employers from ransomware?

The Honorable Gary Palmer (R-AL)

1. Should we be asking the military to do more in these situations? Taking “acts of war” off the table for the moment, how would you advise us to direct our military to bring their awesome powers to bear on the problem of attribution of these hackers and those who control them?
2. In your testimony, you mention that most Critical Infrastructure companies are underfunded in the area of Operational Technology and the ability to monitor and detect attacks there. Do you believe that a mid-sized energy company can reach a level of cybersecurity where they can defend themselves from a motivated state-sponsored attacker? Is that even possible?

¹ *Biden says ransomware attack caused 'minimal damage' to U.S. companies*, Reuters (July 6, 2021).

3. How much of what you would recommend is “companies doing a better job” and how much is “companies fully engaged in (what you called) collective defense” through information sharing? Should we be “doing better” at identifying and eliminating these attackers through whatever means necessary?