SUPPORT

Anton T. Dahbura
Executive Director of the Johns Hopkins University Information Security Institute

Testimony in Support of

House Bill 425 Criminal Law - Crimes Involving Computers
Sponsor: Delegate Erek Barron

Judiciary Committee, February 2, 2021

Thank you, members of the Committee, for the opportunity to testify today. I support House Bill 425 that addresses the possession and use of Ransomware to disrupt the use of computing resources by unauthorized encryption and/or locking of files and other resources.

My name is Anton Dahbura. I am the Executive Director of the Johns Hopkins University Information Security Institute, I am an Associate Research Scientist on the faculty of the Johns Hopkins University Department of Computer Science, and I serve as a member of the Maryland Cybersecurity Council.

My institute has conducted research on the methods used in Ransomware attacks and possible mitigation technologies and strategies. Unfortunately, this continues to be a frustratingly difficult problem to defend against conclusively.

We all know about the devastating Ransomware attack on the City of Baltimore's government computer systems in May 2019, and the more recent Ransomware attack on the Baltimore County Public Schools system last November. But the fact of the matter is that the Ransomware problem is far more catastrophic in scope and scale. Consider the following:

- An inter-agency US whitepaper estimated 4000 attacks *per day* in 2016[1] and is estimated to surpass 8000 attacks per day in 2021[2]
- From June 2015 to June 2016, 79% of businesses surveyed reported at least one ransomware attack[3] and from June 2015 to June 2016, 22% of businesses surveyed reported more than twenty ransomware attacks[4]
- The average cost of a ransomware attack in 2019 was $133,000[5] and the average ransomware payment rose 33% in 2020 over 2019, to $111,605[6]

The Ransomware situation continues to worsen with no end in sight.

Ransomware so pervasive and effective because of its *economic* brilliance and simplicity of Ransomware's design. Ransomware cuts out the middleman in cyber-theft operations, and the simplicity of the required technology enables Ransomware thieves to massively scale up, commoditize, and automate their operations.

The Ransomware technology is so pervasive that turnkey Ransomware packages can be purchased on the Dark Web. Entities that sell them have been known to even provide a 24/7 customer support line! It's little wonder that Ransomware has seen explosive growth with no end in sight.

Based on my understanding of House Bill 425, I believe that it will be an effective law.

HB 425 criminalizes the knowing possession of Ransomware *with the intent to use it*. The twin requirements, knowing about the possession, and with the intent to use it, prevent the Bill from

accidentally criminalizing the activities of law-abiding citizens. And, in the interest of explicitly protecting researchers such those in my institute, the Bill explicitly excludes research purposes from the prohibitions on possession.

Most Ransomware operators is using many different kinds of Ransomware and is regularly testing out new variants. It appears to me that a prosecutor armed with evidence that an operator used *any* Ransomware can now also prosecute them for *all* the different Ransomware they possess. Use of one provides evidence that they knowingly possess and intend to use the others.

My testimony here today is just a brief overview of the Ransomware threat and I hope that it has been helpful to the committee. Based on my knowledge and experience, I support House Bill 425 to strengthen criminal penalties for those that knowingly possess Ransomware with the intent to disrupt the operations of another party's computer system.

To the members of this committee, thank you once again for the opportunity to give testimony here today.

I encourage a favorable report of House Bill 425. Thank you for your consideration.

Addendum to Anton Dahbura's Testimony

References

1. *How to Protect Your Networks from Ransomware*, US inter-agency whitepaper.
2. Ransomware statistics in 2020: From random barrages to targeted hits, DataProt, November 30 2019.
3. *Internet Security Threat Report*, *Ransomware 2017*, Symantec Corporation.
4. Executive Summary, 2018 Internet Security Threat Report, Symantec Corporation.
5. *You May Want to Revise Your Cybersecurity Plan After You See These 2020 Ransomware Statistics!*, ID Agent, July 23, 2020.
6. *The 2020 Cybersecurity stats you need to know*, Fintech News, August 20, 2020.