January 30, 2023

DOJ Multinational Operation to Disrupt Ransomware Organization Focuses on Aiding Ransomware Victims

On January 26, 2023, the U.S. Department of Justice ("DOJ") announced that its months-long effort to disrupt the operations of Hive, a ransomware group that has launched ransomware attacks against more than 1,500 entities around the world, including hospitals, schools, and other critical infrastructure, had resulted in the successful interdiction of the organization's operations.[1] Over the course of its operations against Hive, which commenced in late July 2022, the DOJ employed a combination of strategies to undermine the organization's ransomware operations, including penetrating Hive's computer networks to capture decryption keys and seizing servers and websites used by Hive.[2] The DOJ's successful interdiction of Hive operations is estimated to have saved ransomware victims a total of over $130 million.[3] This most recent operation is a tangible result of the DOJ's concerted effort to fight ransomware, including offensive cyberoperations and cooperation with multiple foreign governments.

Key Takeaways

- **Fighting ransomware with an "all tools" approach continues to be a focus for U.S. law enforcement.** The DOJ's significant efforts to counter Hive's operations reflect the "all tools" approach described by Deputy Attorney General Lisa Monaco in her July 2022 keynote address at the International Conference on Cyber Security.[4] The "tools" used in the Hive operation included "penetrat[ing] Hive's computer networks," "captur[ing] its decryption keys," and seizing the control servers and websites that Hive used, but do not, at least yet, include any public criminal prosecution. Future DOJ efforts to prevent or mitigate ransomware attacks—a high priority for the Department[5]—will likely feature multi-pronged strategies similar to that used against Hive.

- **Victims of ransomware attacks may get more help from law enforcement.** The DOJ's efforts in combating Hive included offering 300 decryption keys to victims who were under attack, saving them $130 million in ransoms, and distributing 1,000 additional decryption keys to previous victims.[6] This assistance to current and former victims of ransomware attacks shows the opportunity for close coordination between private sector companies and U.S. law enforcement, and creates an additional incentive for private sector victims to communicate with law enforcement from the earliest stages of an attack. As DAG

1 *U.S. Department of Justice Disrupts Hive Ransomware Variant*, Department of Justice (Jan. 26, 2023) ("Hive Announcement"), available here.

2 *Id.*

3 *FBI Disrupts 'Hive' Ransomware Group*¸ WALL STREET JOURNAL (Jan. 26, 2023), available here.

4 *Deputy Attorney General Lisa O. Monaco Delivers Keynote Address at International Conference on Cyber Security (ICCS 2022)*, Department of Justice (July 19, 2022), available here.

5 *Strategic Goal 2: Keep Our Country Safe*, Department of Justice, available here.

6 Hive Announcement.

Monaco explained in announcing the operation, the DOJ's action "should speak as clearly to victims of cybercrime as it does to perpetrators," with DOJ "plac[ing] victims at the center of our efforts to mitigate the cyber threat."[7]

The DOJ's Operations against Hive

The Hive ransomware group has targeted more than 1,500 victims around the world since June 2021. Hive's operations followed a ransomware-as-a-service model, which involves the preparation of a "strain" of ransomware software that can be used by various customers to commit ransomware attacks in exchange for a percentage of successful ransom payments—in the case of Hive, administrators received 20 percent of the payment.[8] Hive's ransomware strains were used in what the DOJ described as a "double-extortion" mode of attack, whereby a Hive actor would first expropriate the target's personal data, and then encrypt the target's system.[9] The actor would then demand a ransom from the target, in exchange for both the restoration of the target's access to its systems, and a promise not to publish the target's confidential data.[10] Hive ransomware strains were used in cyberattacks in more than 80 countries, and resulted in more than $100 million in losses associated with ransom payments. The attacks have prominently targeted healthcare providers, with serious consequences for medical systems already overwhelmed by the COVID-19 pandemic.[11]

The DOJ's actions against Hive relied on extensive international cooperation. The Department explained that the seizure of Hive's servers and websites was a joint operation involving the German Federal Criminal Police and Reutlingen Police Headquarters-CID Esslingen and the Netherlands National High Tech Crime Unit.[12] The DOJ received more general assistance from law enforcement agencies in nine other countries, including Canada, France, the United Kingdom, and Norway.[13]

The scale of the economic harm both threatened and actually caused by Hive is illustrative of the broader threat posed by ransomware. A 2021 study commissioned by the Cybersecurity and Infrastructure Security Agency determined that ransomware attacks had been conducted against 14 of the 16 infrastructure sectors designated by the federal government as "critical," including defense, food and agriculture, and emergency services.[14] Another study by the Financial Crimes Enforcement Network estimated the total cost of ransomware attacks committed against American entities in 2021 to be roughly $900 million.[15]

We will continue to provide updates on developments in cyber threats.

* * *

7 Hive Announcement.

8 *Id.*

9 *Id.*

10 *Id.*

11 *FBI seizes website used by notorious ransomware gang*, CNN (Jan. 26, 2023), available here.

12 *Id.*

13 *Id.*

14 *2021 Trends Show Increased Globalized Threat of Ransomware*, Cybersecurity and Infrastructure Security Agency (Feb. 10, 2022), available here.

15 *Financial Trend Analysis*, Financial Crimes Enforcement Network (Nov. 1, 2022), available here.

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

David K. Kessler
+1-212-373-3614
dkessler@paulweiss.com

Associate Neil Chitrao contributed to this Client Memorandum.