U.S. Department of Justice

Office of the Deputy Attorney General

Washington, D.C. 20530

April 20, 2021

MEMORANDUM FOR HEADS OF DEPARTMENT LITIGATING COMPONENTS
ALL UNITED STATES ATTORNEYS
FEDERAL BUREAU OF INVESTIGATION

FROM: John P. Carlin JPC
Acting Deputy Attorney General

SUBJECT: Ransomware and Digital Extortion Task Force

Malicious cyber actors increasingly target U.S. businesses and their networks to perpetuate digital extortion, including through the use of ransomware. These criminals work to infect systems with malware designed to block a victim's access to its own data and then demand that the victim pay a ransom in order to regain access to its data. Cyber criminals also separately extort victims with the threat of publicly releasing stolen data unless a ransom is paid.

Ransomware can have devastating human and financial consequences. When criminals target critical infrastructure such as hospitals, utilities, and municipal networks, their activity jeopardizes the safety and health of Americans. This criminal activity also has an increasing economic toll on U.S. companies, with 2020 being the worst year to date for ransomware attacks. Ransom demands made to victims averaged over $100,000 and in some cases were up to tens of millions of dollars. Ransomware and other forms of digital extortion are estimated to have caused billions of dollars in damages last year alone. These digital attacks appear to be most often deployed by transnational criminal enterprises seeking to reap financial rewards from their cybercriminal activities. In certain instances, the Department's investigations have identified hackers within these enterprises as having nation-state ties.

As part of its commitment to fighting cybercrime in all forms, the Department has prosecuted those responsible for the spread of some of the most widespread and pernicious strains of ransomware, as well as disrupted infrastructure used in cyber-extortion schemes. These successful efforts include charges and seizures related to the NetWalker ransomware strain; the indictment of two Iranian nationals for deploying SamSam ransomware against the cities of Atlanta and Newark, as well as more than 200 other victims; and the recent disruption of the

Emotet botnet, used to infect hundreds of thousands of computers throughout the United States with various types of malware, including ransomware, which caused hundreds of millions of dollars of damage worldwide. The Department has also brought charges stemming from digital extortion and ransomware activity against cyber actors linked to nation-state threats, such as the North Korean regime-backed hacking team responsible for the development of WannaCry 2.0; and a Russian national responsible for the propagation of the Bugat or Dridex malware, who is now subject to U.S. sanctions in connection with assistance rendered to the Russian government.[1]

THE RANSOMWARE AND DIGITAL EXTORTION TASK FORCE

Although the Department has taken significant steps to address cybercrime, it is imperative that we bring the full authorities and resources of the Department to bear to confront the many dimensions and root causes of this threat. Today, we announce the establishment of the Ransomware and Digital Extortion Task Force (herein the "Task Force"), to include the Criminal Division, the National Security Division, the Executive Office of United States Attorneys, the Civil Division, and the Federal Bureau of Investigation.[2] To ensure that we are focused and coordinated in our efforts to fight digital extortion, the Task Force will aim to position the Department to comprehensively and most effectively address this pervasive cyber threat by using all of its available tools.

Enhancing the Department's Capability to Disrupt, Investigate, and Prosecute Ransomware Attacks: First, in an effort led by the Criminal Division, working with the United States Attorney's Offices, the Task Force will work to ensure that the Department prioritizes the disruption, investigation, and prosecution of ransomware and digital extortion activity by tracking and dismantling the development and deployment of malware, identifying the cybercriminals responsible, and holding those individuals accountable. This will include (1) increased training and resources dedicated to addressing the threat; (2) a greater focus on intelligence and lead sharing across the Department; (3) leveraging of all sources of investigative leads, including the use of human sources and identifying links between criminal actors and nation-states; and (4) efforts to improve coordination across the Department's components and U.S. Attorney's Offices.

---

[1] *See* Press Release, Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware, Dec. 5, 2019 (*available at* https://home.treasury.gov/news/press-releases/sm845).

[2] The work of the Task Force will be informed by the expertise of the Computer Crime and Intellectual Property Section (CCIPS); the National Security Division's Counterintelligence and Export Control Section (CES), the Office of International Affairs (OIA); the Money Laundering and Asset Recovery Section (MLARS), and the National Cyber Investigative Joint Task Force (NCIJTF). The Department's Chief Information Officer will also inform the work of the Task Force, as appropriate.

Targeting the Ransomware Criminal Ecosystem as a Whole: Second, the Task Force will design and implement a strategy to disrupt and dismantle the criminal ecosystem used by malign actors to perpetuate digital extortion attacks, as well as the means by which these actors monetize and launder the proceeds of their extortion schemes. This will include the use of all available criminal, civil, and administrative actions for enforcement, ranging from takedowns of servers used to spread ransomware to seizures of these criminal enterprises' ill-gotten gains. The Task Force will also ensure that the Department focuses upon the online services that allow these digital extortion schemes to persist, such as online forums that advertise the sale of ransomware or provide communication platforms to further the extortion and hosting services that knowingly facilitate these attacks.

Strengthening Public-Private Partnerships: Third, the Task Force will work to strengthen and enhance partnerships between the Department and private industry across a wide range of sectors to address ransomware and digital extortion. For example, the Task Force will examine ways the Department can encourage organizations to come forward and notify the Department if and when they become victims in order for the government to investigate and provide information that enables effective incident response and remediation. To foster and encourage further information sharing, these efforts will build upon existing relationships between the Department and private sector companies such as major online service providers, threat intelligence firms, and insurance firms whose clients are victimized by these schemes.

Working in Tandem with Federal Partners: Fourth, because combating the growing threat of ransomware and digital extortion demands a whole-of-government approach, the Task Force will work with many of our key federal partners, such as the U.S. Department of Homeland Security, including the U.S. Secret Service and the Cybersecurity and Infrastructure Security Agency (CISA); the U.S. Department of Treasury, including the Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN); the U.S. Department of Defense; the U.S. Department of Commerce, and others. Coordination of these efforts will ensure that the whole of the U.S. government's resources may be brought to bear to address these threats in a systematic and comprehensive way, to heighten the risks and decrease the rewards for those engaging in digital extortion.

Furthering International Collaboration: Fifth, the Task Force will work to further collaboration with our foreign partners to share information and coordinate efforts in combating and mitigating the ransomware and digital extortion threat. Because many of the cyber actors responsible for these crimes, infrastructure used to facilitate these digital extortion attacks, and victims of these schemes are located overseas, close cooperation with our foreign partners has been and will continue to be crucial to successfully identify those responsible for malicious digital extortion, to dismantle the criminal enterprises' ongoing operations, and to advance opportunities to disrupt safe havens for such malicious activity.

The Task Force seeks to incorporate and augment existing efforts by the Department to combat cybercrime, while recognizing the unique challenges that ransomware and digital extortion pose. The Task Force will bring all of the Department's resources to bear to bolster our all-tools approach and work with our partners here and abroad to combat the threat of ransomware and digital extortion, and to ensure that we hold those who participate in the propagation of these crimes responsible and accountable.