United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510–6275

VIA ELECTRONIC TRANSMISSION

July 30, 2020

The Honorable Christopher Wray
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue NW
Washington, DC 20535

The Honorable Christopher Krebs
Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
245 Murray Lane
Washington, DC 20528

Dear Directors Wray and Krebs:

We write you today regarding recent cyberattacks by Russian actors, specifically NetWalker and its ransomware cyberattacks. NetWalker uses a sophisticated ransomware that usurps an individual's private or sensitive software data through their e-mail or ransomware-as-a-service (RaaS). NetWalker threatens users with the publication of their data and adds an encryption that makes it impossible for users to recover their data without paying the ransom. As you both know, normal ransomware attacks would only steal data and request a ransom payment, but would not encrypt the data.

According to public reports, NetWalker has been traced back to Russian government-affiliated hackers. The RaaS attack is one that has long been used by Russian actors. There has also been an increase of Russian-language Dark Web forum posts recruiting individuals to the NetWalker group that recommend experience in RaaS cyberattacks and previous access to company networks.

In recent months there have been multiple NetWalker attacks on education systems, medical facilities, businesses, and government agencies. In March 2020, Champaign-Urbana Public Health District (CUPHD) was attacked by NetWalker. This attack caused a disruption in the

CUPHD's ability to access patient records for patients with COVID-19.[1] Similarly, on June 1, 2020, the University of California, San Francisco (UCSF), reported paying a $1.14 million dollar ransom. According to UCSF officials, the NetWalker group stole and encrypted medical and academic research from UCSF.[2]

The Philadelphia-area Crozer-Keystone Health System also reported a NetWalker attack in June during ongoing treatment of COVID-19 patients. The Philadelphia health system stated that NetWalker stole financial information data that was later posted on the NetWalker blog.[3] We are also aware of at least one North Carolina company that has been targeted – and we suspect there may be many more.

On July 16, 2020, a joint advisory was released by the United States, Canada, and the United Kingdom alerting the public to the latest COVID-19 cyberattacks. According to the advisory, these hackers attempted to steal COVID-19 related intellectual property (IP). The attack, which was intended to disrupt, create mistrust, and steal IP, is one that has been used by Russian Intelligence groups Fancy Bear and Cozy Bear before. According to reports, these Russian Intelligence groups continue to launch attacks intended to undermine and disrupt the critical COVID-19 research that is needed to save lives. These attacks are a risk to public safety and to our national security.

We believe that these latest cyberattacks by Russian government affiliated hackers makes awareness and increased cybersecurity and guidance on how the public and private sector should protect their data essential. We appreciate the steps your agencies have taken to combat these attacks by Russian-affiliated hackers and similar attacks by hackers affiliated with the Chinese government. To better understand the types of attacks being launched by these hackers and the efforts by your agencies to raise awareness about the threat of these attacks, please provide answers to the following questions by no later than August 30, 2020.

1. Has the number of NetWalker attacks generally increased during the COVID-19 pandemic? What sorts of businesses and institutions does NetWalker target? Please provide specific data where possible.
2. What additional steps are CISA and the FBI taking to counter or prevent the NetWalker attacks?
3. Which other foreign actors, besides Russia, are conducting attacks using RaaS similar to NetWalker attacks?

[1] Jessica Davis, *Illinois Public Health Website Hit With Ransomware Amid Coronavirus,* HealthITSecurity, (July 20, 2020), https://healthitsecurity.com/news/illinois-public-health-website-hit-with-ransomware-amid-coronavirus.

[2] University of California San Francisco: Campus News, *Update on IT Security Incident at UCSF,* University of California San Francisco (July 21, 2020), https://www.ucsf.edu/news/2020/06/417911/update-it-security-incident-ucsf.

[3] DataBreaches, Pennsylvania health system hit by NetWalker ransomware, DataBreaches.Net (July 20, 2020), https://www.databreaches.net/pennsylvania-health-system-hit-by-netwalker-ransomware/.

4. Has there been a rise in NetWalker recruitment posts during COVID-19? What steps are being taken to shut down these posts?
5. What has the DOJ and CISA done to increase awareness about the risk of NetWalker for research facilities, health departments, universities, and businesses during the COVID-19 pandemic?
6. What additional funding or legislative authority would you recommend Congress enact to increase your ability to effectively combat sophisticated actors such as NetWalker?

Thank you for your prompt attention to this matter. Please know that as you continue to combat state-sponsored hacking and the theft of American intellectual property we stand ready and willing to assist you. If you have any questions, please do not hesitate to contact us.

Sincerely,

Thom Tillis

Thom Tillis
United States Senator

John Cornyn

John Cornyn
United States Senator