$590 mn in ransomware payments reported to US in 2021 as attacks surge

15 October 2021, by Joshua Melvin

New data showed a major jump in the number of ransomware-related payments that have been reported to US authorities.

New data out Friday showed $590 million in ransomware-related payments were reported to US authorities in the first half of 2021 alone, setting a pace to beat totals for the whole previous decade as cyber-extortion booms.

The figure is also 42 percent higher than the amount divulged by financial institutions for all of 2020, the US Treasury report said, and there are strong indicators the true cost could be in the billions.

"If current trends continue, (reports) filed in 2021 are projected to have a higher ransomware-related transaction value than... filed in the previous 10 years combined," said Treasury's Financial Crimes Enforcement Network.

The heists involve breaking into a company or institution's network to encrypt its data, then demanding a ransom, typically paid via cryptocurrency in exchange for the digital key to unlock it.

Washington has sought to crack down on a sharp rise in attacks, including issuing its first sanctions against an online exchange where illicit operators have allegedly swapped cryptocurrency for cash.

Recent assaults on a major US oil pipeline, a meatpacking company and the Microsoft Exchange email system drew attention to the vulnerability of US infrastructure to digital pirates who are extorting staggering sums.

Treasury said investigators found over 150 online wallets for cyptocurrency and by analyzing them uncovered roughly $5.2 billion in transactions potentially tied to ransomware payments.

Companies and institutions face intense pressure to pay up in order to get their data unlocked, but also to keep the attack from potentially angry clients and authorities who issue stern warnings not to give cash to criminals.

Threat to critical infrastructure

The report, based on the suspicious activity alerts that financial firms have to file, noted it was unclear if the jump represented increased awareness of the cybercrime.

"This trend potentially reflects the increasing overall prevalence of ransomware-related incidents as well as improved detection and reporting," Treasury said.

The victims of the attacks were not identified in the report, which noted some of the apparent ransoms were paid before January 2021.

The new data on the scale of payments related to hacks came after more than two dozen nations resolved to collectively fight ransomware during a Washington-led summit.

The United States gathered the countries—with the

notable exception of Russia—to unify and boost efforts to fight a cybercrime that is transnational, on the rise and potentially devastating.

Stronger digital security and offline backups as well as collectively targeting the laundering of the attacks' proceeds were identified as crucial steps in the fight.

"We will consider all national tools available in taking action against those responsible for ransomware operations threatening critical infrastructure and public safety," the nations said in a joint statement.

Great Britain, Australia, India, Japan, France, Germany, South Korea, the European Union, Israel, Kenya, Mexico, and others were among those that joined in the virtual gathering on Wednesday and Thursday.

During the summit, nations recounted their agonizing experiences with cyber-extortion, including a digital "disaster" declaration in Germany and Israel even announcing a blitz was underway against a major hospital.