Microsoft Exchange hack caused by China, US and allies say

July 19 2021, by Eric Tucker

In this Jan. 28, 2020, file photo, a Microsoft computer is among items displayed at a Microsoft store in suburban Boston. The Biden administration on Monday, July 19, 2021, blamed China for a hack of Microsoft Exchange email server software that compromised tens of thousands of computers around the world earlier in the year. (AP Photo/Steven Senne, File

The Biden administration and Western allies formally blamed China on Monday for a massive hack of Microsoft Exchange email server software and asserted that criminal hackers associated with the Chinese government have carried out ransomware and other illicit cyber operations.

The announcements, though not accompanied by sanctions against the Chinese government, were intended as a forceful condemnation of activities a senior Biden administration official described as part of a "pattern of irresponsible behavior in cyberspace." They highlighted the ongoing threat from Chinese hackers even as the administration remains consumed with trying to curb ransomware attacks from Russia-based syndicates that have targeted critical infrastructure.

The broad range of cyberthreats from Beijing disclosed on Monday included a ransomware attack from government-affiliated hackers that targeted victims—including in the U.S.—with demands for millions of dollars. U.S officials also alleged that criminal contract hackers associated with China's Ministry of State Security have engaged in cyber extortion schemes and theft for their own profit.

Meanwhile, the Justice Department on Monday announced charges against four Chinese nationals who prosecutors said were working with the MSS in a hacking campaign that targeted dozens of computer systems, including companies, universities and government entities. The defendants are accused of targeting trade secrets and confidential business information, including scientific technologies and infectious-disease research.

Unlike in April, when public finger-pointing of Russian hacking was paired with a raft of sanctions against Moscow, the Biden administration did not announce any actions against Beijing. Nonetheless, a senior administration official who briefed reporters said that the U.S. has

confronted senior Chinese officials and that the White House regards the multination shaming as sending an important message, even if no single action can change behavior.

President Joe Biden told reporters "the investigation's not finished," and White House press secretary Jen Psaki did not rule out future consequences for China, saying, "This is not the conclusion of our efforts as it relates to cyber activities with China or Russia."

Even without fresh sanctions, Monday's actions are likely to exacerbate tensions with China at a delicate time. Just last week, the U.S. issued separate stark warnings against transactions with entities that operate in China's western Xinjiang region, where China is accused of repressing Uyghur Muslims and other minorities.

The administration also advised American firms of the deteriorating investment and commercial environment in Hong Kong, where China has been cracking down on democratic freedoms it had pledged to respect in the former British colony.

The European Union and Britain were among the allies who called out China. The EU said malicious cyber activities with "significant effects" that targeted government institutions, political organizations and key industries in the bloc's 27 member states could be linked to Chinese hacking groups. The U.K.'s National Cyber Security Centre said the groups targeted maritime industries and naval defense contractors in the U.S. and Europe and the Finnish parliament.

In a statement, EU foreign policy chief Josep Borrell said the hacking was "conducted from the territory of China for the purpose of intellectual property theft and espionage."

The Microsoft Exchange cyberattack "by Chinese state-backed groups

was a reckless but familiar pattern of behaviour," U.K. Foreign Secretary Dominic Raab said.

NATO, in its first public condemnation of China for hacking activities, called on Beijing to uphold its international commitments and obligations "and to act responsibly in the international system, including in cyberspace." The alliance said it was determined to "actively deter, defend against and counter the full spectrum of cyber threats."

That hackers affiliated with the Ministry of State Security were engaged in ransomware was surprising and concerning to the U.S. government, the senior administration official said. But the attack, in which an unidentified American company received a high-dollar ransom demand, also gave U.S. officials new insight into what the official said was "the kind of aggressive behavior that we're seeing coming out of China."

A spokesperson for the Chinese Embassy in Washington, Liu Pengyu, said in a statement that the "U.S. has repeatedly made groundless attacks and malicious smear against China on cybersecurity. Now this is just another old trick, with nothing new in it." The statement called China "a severe victim of the US cyber theft, eavesdropping and surveillance."

The majority of the most damaging and high-profile recent ransomware attacks have involved Russian criminal gangs. Though the U.S. has sometimes seen connections between Russian intelligence agencies and individual hackers, the use of criminal contract hackers by the Chinese government "to conduct unsanctioned cyber operations globally is distinct," the official said.

Dmitri Alperovitch, the former chief technology officer of the cybersecurity firm Crowdstrike, said the announcement makes clear that MSS contractors who for years have worked for the government and conducted operations on its behalf have over time decided—either with

the approval or the "blind eye of their bosses"—to "start moonlighting and engaging in other activities that could put money in their pockets."

The Microsoft Exchange hack that months ago compromised tens of thousands of computers around the world was swiftly attributed to Chinese cyber spies by Microsoft.

An administration official said the government's attribution to hackers affiliated with the Ministry of State Security took until now in part because of the discovery of the ransomware and for-profit hacking operations and because the administration wanted to pair the announcement with guidance for businesses about tactics that the Chinese have been using.

Given the scope of the attack, Alperovitch said it was "puzzling" that the U.S. did not impose sanctions.

"They certainly deserve it, and at this point, it's becoming a glaring standout that we have not," he said.

He added, in a reference to a large Russian cyberespionage operation discovered late last year, "There's no question that the Exchange hacks have been more reckless, more dangerous and more disruptive than anything the Russians have done in SolarWinds.