0-NPR-Biden Administration

An alert on a suspected attack by state-backed Chinese hackers from the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency in April. Jon Elswick/AP hide caption

toggle caption

Jon Elswick/AP

An alert on a suspected attack by state-backed Chinese hackers from the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency in April.

Jon Elswick/AP

The White House is publicly blaming China for an attack on Microsoft’s Exchange email server software that compromised tens of thousands of computers worldwide, allowing hackers to gain access to troves of sensitive data.

Separately, the Department of Justice announced Monday that a federal grand jury in May had indicted Chinese nationals accused of working with official sanction from Beijing to break into computer systems belonging to U.S. companies, universities and governments.

The cyberattack on Microsoft, which is believed to have begun in January , reportedly injected computers with malware that secretly monitored systems belonging to small businesses, local and state governments and some military contractors.

As part of the attack, an unidentified American company was also hit with a high-dollar ransom demand, according to a senior Biden administration official.

U.S. allies are also blaming China for cyberattacks

The official, who briefed reporters late Sunday, said the U.S. would be joined by the European Union, the United Kingdom, Australia, Canada, New Zealand, Japan and NATO in condemning Beijing's Ministry of State Security for the malicious cyberattacks.

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

U.K. Foreign Secretary Dominic Raab said China's actions represent "a reckless but familiar pattern of behavior."

"The Chinese Government must end this systematic cyber sabotage and can expect to be held [to] account if it does not," Raab said in a statement .

In a tweet , NATO Secretary General Jens Stoltenberg said that the alliance "stands in solidarity with all those affected by malicious cyber activities, including the Microsoft Exchange Server compromise. We call on all states, including China, to uphold their international obligations & act responsibly."

The announcements follow heightened concern over ransomware attacks that the White House has blamed on Russian hackers and highlights how the West's traditional Cold War rivals have stepped up pressure in cyberspace in recent years.

Hacks Are Prompting Calls For A Cyber Agreement, But Reaching One Would Be Tough

The White House says China worked with criminal contract hackers

The Biden administration official said that China's Ministry of State Security employed criminal contract hackers "to conduct unsanctioned cyber operations globally, including for their own personal profit."

Although the U.S. says criminal gangs of hackers with links to Russian intelligence carried out such audacious ransomware attacks as the one that caused Colonial Pipeline – a major U.S. petroleum distribution network – to

shut down temporarily, China's outright hiring of contract hackers is "distinct," the official said.

In Wake Of Colonial Attack, Pipelines Now Must Report Cybersecurity Breaches

"The United States has long been concerned about the People's Republic of China's irresponsible and destabilizing behavior in cyberspace," the official said. Such hacks pose a serious economic and national security threat to the U.S. and its allies, the official said.

"Their operations include criminal activities, such as cyber-enabled extortion, crypto-jacking and theft from victims around the world for financial gain. In some cases, we're aware of reports that PRC government-affiliated cyber operators have conducted ransomware operations against private companies that have included ransom demands of millions of dollars," the official said.

Although no sanctions against China have been announced, the U.S. has "raised its concerns" with Beijing, the official said. "The first important piece is the publicly calling out the pattern of irresponsible malicious cyberactivity, and doing it with allies and partners."

Previously, a spokesperson for China's Foreign Ministry has said that Beijing "firmly opposes and combats cyberattacks and cyber theft in all forms" and cautioned against "groundless accusations" that China is involved in such attacks, according to The Associated Press.

Four Chinese nationals have been indicted

However, on Monday, the Department of Justice said in a statement that a federal grand jury in San Diego had indicted four nationals and residents of China with "a campaign to hack into the computer systems of dozens of victim companies, universities and government entities in the United States and abroad between 2011 and 2018."

The indictment, unsealed Friday, alleges a conspiracy to steal data with a "significant economic benefit to China's companies and commercial

sectors, including information that would allow the circumvention of lengthy and resource-intensive research and development processes."

The four individuals worked with China's Hainan State Security Department "to obfuscate the Chinese government's role in such theft by establishing a front company, Hainan Xiandun Technology Development Co., Ltd.," which has since been dismantled, the Justice Department said.

The FBI, National Security Agency and the U.S. Cybersecurity and Infrastructure Security Agency issued a joint advisory Monday laying out ways that government agencies and businesses could protect themselves from such attacks.