BRIEFING ROOM

The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China

JULY 19, 2021 • STATEMENTS AND RELEASES

The United States has long been concerned about the People's Republic of China's (PRC) irresponsible and destabilizing behavior in cyberspace. Today, the United States and our allies and partners are exposing further details of the PRC's pattern of malicious cyber activity and taking further action to counter it, as it poses a major threat to U.S. and allies' economic and national security.

An unprecedented group of allies and partners – including the European Union, the United Kingdom, and NATO – are joining the United States in exposing and criticizing the PRC's malicious cyber activities.

The PRC's pattern of irresponsible behavior in cyberspace is inconsistent with its stated objective of being seen as a responsible leader in the world. Today, countries around the world are making it clear that concerns regarding the PRC's malicious cyber activities is bringing them together to call out those activities, promote network defense and cybersecurity, and act to disrupt threats to our economies and national security.

Our allies and partners are a tremendous source of strength and a unique American advantage, and our collective approach to cyber threat information sharing, defense, and mitigation helps

hold countries like China to account. Working collectively enhances and increases information sharing, including cyber threat intelligence and network defense information, with public and private stakeholders and expand diplomatic engagement to strengthen our collective cyber resilience and security cooperation. Today's announcement builds on the progress made from the President's first foreign trip. From the G7 and EU commitments around ransomware to NATO adopting a new cyber defense policy for the first time in seven years, the President is putting forward a common cyber approach with our allies and laying down clear expectations and markers on how responsible nations behave in cyberspace.

Today, in coordination with our allies, the Biden administration is:

Exposing the PRC's use of criminal contract hackers to conduct unsanctioned cyber operations globally, including for their own personal profit.

The United States is deeply concerned that the PRC has fostered an intelligence enterprise that includes contract hackers who also conduct unsanctioned cyber operations worldwide, including for their own personal profit. As detailed in public charging documents unsealed in October 2018 and July and September 2020, hackers with a history of working for the PRC Ministry of State Security (MSS) have engaged in ransomware attacks, cyber enabled extortion, crypto-jacking, and rank theft from victims around the world, all for financial gain.

In some cases, we are aware that PRC government-affiliated cyber operators have conducted ransomware operations against private companies that have included ransom demands of millions of dollars. The PRC's unwillingness to address criminal activity by contract hackers harms governments, businesses, and critical infrastructure operators through billions of dollars in lost intellectual property, proprietary information, ransom payments, and mitigation efforts.

[United States Department of Justice] imposing costs and announcing criminal charges against four MSS hackers.

The US Department of Justice is announcing criminal charges against four MSS hackers addressing activities concerning a multiyear campaign targeting foreign governments and

entities in key sectors, including maritime, aviation, defense, education, and healthcare in a least a dozen countries. DOJ documents outline how MSS hackers pursued the theft of Ebola virus vaccine research and demonstrate that the PRC's theft of intellectual property, trade secrets, and confidential business information extends to critical public health information. Much of the MSS activity alleged in the Department of Justice's charges stands in stark contrast to the PRC's bilateral and multilateral commitments to refrain from engaging in cyber-enabled theft of intellectual property for commercial advantage.

Attributing with a high degree of confidence that malicious cyber actors affiliated with PRC's MSS conducted cyber espionage operations utilizing the zero-day vulnerabilities in Microsoft Exchange Server disclosed in early March 2021.

Before Microsoft released its security updates, MSS-affiliated cyber operators exploited these vulnerabilities to compromise tens of thousands of computers and networks worldwide in a massive operation that resulted in significant remediation costs for its mostly private sector victims.

We have raised our concerns about both this incident and the PRC's broader malicious cyber activity with senior PRC Government officials, making clear that the PRC's actions threaten security, confidence, and stability in cyberspace.

The Biden Administration's response to the Microsoft Exchange incident has strengthened the USG's Cyber Defenses.

In the past few months, we have focused on ensuring the MSS-affiliated malicious cyber actors were expelled from public and private sector networks and the vulnerability was patched and mitigated to prevent the malicious cyber actors from returning or causing additional damage.

- As announced in April, the U.S. Government conducted cyber operations and pursued proactive network defense actions to prevent systems compromised through the Exchange Server vulnerabilities from being used for ransomware attacks or other malicious purposes. The United States will continue to take all appropriate steps to

protect the American people from cyber threats. Following Microsoft's original disclosure in early March 2021, the United States Government also identified other vulnerabilities in the Exchange Server software. Rather than withholding them, the United States Government recognized that these vulnerabilities could pose systemic risk and the National Security Agency notified Microsoft to ensure patches were developed and released to the private sector. We will continue to prioritize sharing vulnerability information with the private sector to secure the nation's networks and infrastructure.

- The U.S. Government announced and operated under a new model for cyber incident response by including private companies in the Cyber Unified Coordination Group (UCG) to address the Exchange Server vulnerabilities. The UCG is a whole-of-government coordination element stood up in response to a significant cyber incident. We credit those companies for being willing to collaborate with the United States Government in the face of a significant cyber incident that could have been substantially worse without key partnership of the private sector. We will build on this model to bolster public-private collaboration and information sharing between the United States Government and the private sector on cybersecurity.

- Today, the National Security Agency, the Cybersecurity and Infrastructure Agency, and the Federal Bureau of Investigation released a cybersecurity advisory to detail additional PRC state-sponsored cyber techniques used to target U.S. and allied networks, including those used when targeting the Exchange Server vulnerabilities. By exposing these techniques and providing actionable guidance to mitigate them, the U.S. Government continues to empower network defenders around the world to take action against cybersecurity threats. We will continue to provide such advisories to ensure companies and government agencies have actionable information to quickly defend their networks and protect their data.

The Biden Administration is working around the clock to modernize Federal networks and improve the nation's cybersecurity, including of critical infrastructure.

- The Administration has funded five cybersecurity modernization efforts across the Federal government to modernize network defenses to meet the threat. These include state-of-the-art endpoint security, improving logging practices, moving to a secure

cloud environment, upgrading security operations centers, and deploying multi-factor authentication and encryption technologies.

- The Administration is implementing President Biden's Executive Order to improve the nation's cybersecurity and protect Federal government networks. The E.O. contains aggressive but achievable implementation milestones, and to date we have met every milestone on time including:

    - The National Institute of Standards and Technology (NIST) convened a workshop with almost 1000 participants from industry, academia, and government to obtain input on best practices for building secure software.

    - NIST issued guidelines for the minimum standards that should be used by vendors to test the security of their software. This shows how we are leveraging federal procurement to improve the security of software not only used by the federal government but also used by companies, state and local governments, and individuals.

    - The National Telecommunications and Information Administration (NTIA) published minimum elements for a Software Bill of Materials, as a first step to improve transparency of software used by the American public.

    - The Cybersecurity and Infrastructure Security Agency (CISA) established a framework to govern how Federal civilian agencies can securely use cloud services.
- We continue to work closely with the private sector to address cybersecurity vulnerabilities of critical infrastructure. The Administration announced an Industrial Control System Cybersecurity Initiative in April and launched the Electricity Subsector Action Plan as a pilot. Under this pilot, we have already seen over 145 of 255 priority electricity entities that service over 76 million American customers adopt ICS cybersecurity monitoring technologies to date, and that number keeps growing. The Electricity Subsector pilot will be followed by similar pilots for pipelines, water, and chemical.

- The Transportation Security Administration (TSA) issued Security Directive 1 to require critical pipeline owners and operators to adhere to cybersecurity standards. Under this directive, those owners and operators are required to report confirmed and potential cybersecurity incidents to CISA and to designate a Cybersecurity Coordinator, to be available 24 hours a day, seven days a week. The directive also requires critical pipeline owners and operators to review their current practices as well as to identify any gaps and related remediation measures to address cyber-related risks and report the results to TSA and CISA within 30 days. In days to come, TSA will issue Security Directive 2 to further support the pipeline industry in enhancing its cybersecurity and that strengthen the public-private partnership so critical to the cybersecurity of our homeland.

By exposing the PRC's malicious activity, we are continuing the Administration's efforts to inform and empower system owners and operators to act. We call on private sector companies to follow the Federal government's lead and take ambitious measures to augment and align cybersecurity investments with the goal of minimizing future incidents.

###