The New York Times

# *Preparing for Retaliation Against Russia, U.S. Confronts Hacking by China*

The proliferation of cyberattacks by rivals is presenting a challenge to the Biden administration as it seeks to deter intrusions on government and corporate systems.

Jake Sullivan, President Biden’s national security adviser, last month. He said on Thursday that the White House was “closely tracking” reports that the vulnerabilities exploited in the Microsoft hacking were being used in “potential compromises of U.S. think tanks and defense industrial base entities.”Credit...Stefani Reynolds for The New York Times

**By David E. Sanger, Julian E. Barnes and Nicole Perlroth**

- March 7, 2021

WASHINGTON — Just as it plans to begin retaliating against Russia for the large-scale hacking of American government agencies and corporations discovered late last year, the Biden administration faces a new cyberattack that raises the question of whether it will have to strike back at another major adversary: China.

Taken together, the responses will start to define how President Biden fashions his new administration's response to escalating cyberconflict and whether he can find a way to impose a steeper penalty on rivals who regularly exploit vulnerabilities in government and corporate defenses to spy, steal information and potentially damage critical components of the nation's infrastructure.

The first major move is expected over the next three weeks, officials said, with a series of clandestine actions across Russian networks that are intended to be evident to President Vladimir V. Putin and his intelligence services and military but not to the wider world.

The officials said the actions would be combined with some kind of economic sanctions — though there are few truly effective sanctions left to impose — and an executive order from Mr. Biden to accelerate the hardening of federal government networks after the Russian hacking, which went undetected for months until it was discovered by a private cybersecurity firm.

The issue has taken on added urgency at the White House, the Pentagon and the intelligence agencies in recent days after the public exposure of a major breach in Microsoft email systems used by small businesses, local governments and, by some accounts, key military contractors.

Microsoft identified the intruders as a state-sponsored Chinese group and moved quickly to issue a patch to allow users of its software to close off the vulnerability.

But that touched off a race between those responsible for patching the systems and a raft of new attackers — including multiple other Chinese hacking groups, according to Microsoft — who started using the same exploit this week.

The United States government has not made public any formal determination of who was responsible for the hacking, but at the White House and on Microsoft's campus in Redmond, Wash., the fear is that espionage and theft may be a prelude to far more destructive activity, such as changing data or wiping it out.

The White House underscored the seriousness of the situation in a statement on Sunday from the National Security Council.

“The White House is undertaking a whole of government response to assess and address the impact” of the Microsoft intrusion, the statement said. It said the response was being led by Anne Neuberger, a former senior National Security Agency official who is the first occupant of a newly created post: deputy national security adviser for cyber and emerging technologies.

The statement said that national security officials were working throughout the weekend to address the hacking and that “this is an active threat still developing, and we urge network operators to take it very seriously.”

Jake Sullivan, Mr. Biden’s national security adviser, said on Twitter on Thursday that the White House was “closely tracking” the reports that the vulnerabilities in Microsoft Exchange were being used in “potential compromises of U.S. think tanks and defense industrial base entities.”

The discovery came as Mr. Biden’s national security team, led by Mr. Sullivan and Ms. Neuberger, has moved to the top of its agenda an effort to deter attacks, whether their intent is theft, altering data or shutting down networks entirely. For the president, who promised that the Russian attack would not “go unanswered,” the administration’s reactions in the coming weeks will be a test of his ability to assert American power in an often unseen but increasingly high-stakes battle among major powers in cyberspace.

A mix of public sanctions and private actions is the most likely combination to force a “broad strategic discussion with the Russians,” Mr. Sullivan said in an interview on Thursday, before the scope of the Chinese attack was clear.

“I actually believe that a set of measures that are understood by the Russians, but may not be visible to the broader world, are actually likely to be the most effective measures in terms of clarifying what the United States believes are in bounds and out of bounds, and what we are prepared to do in response,” he added.

From the first day of the new administration, Mr. Sullivan has been reorganizing the White House to fashion such responses. The same order he issued on Jan. 20, requiring the military to advise the White House before conducting drone strikes outside war zones, contained a paragraph with separate instructions for dealing with major cyberoperations that risk escalating conflict.

The order left in place, however, a still secret document signed by President Donald J. Trump in August 2018 giving the United States Cyber Command broader authorities than it had during the Obama administration to conduct day-to-day, short-of-war skirmishes in cyberspace, often without explicit presidential authorization.

Under the new order, Cyber Command will have to bring operations of significant size and scope to the White House and allow the National Security Council to review or adjust those operations, according to officials briefed on the memo. The forthcoming operation against Russia, and any potential response to China, is likely to fall in this category.

The hacking that Microsoft has attributed to China poses many of the same challenges as the SolarWinds attack by the Russians that was discovered late last year.Credit...Swayne B. Hall/Associated Press

American officials continue to try to better understand the scope and damage done by the Chinese attack, but every day since its revelation has suggested that it is bigger, and potentially more harmful, than first thought.

“This is a crazy huge hack,” Christopher C. Krebs, the former director of the Cybersecurity and Infrastructure Security Agency, wrote on Twitter on Friday.

The initial estimates were that 30,000 or so systems were affected, mostly those operated by businesses or government agencies that use Microsoft software and run their email systems in-house. (Email and others systems run on Microsoft’s cloud were not affected.)

But the breadth of the intrusion and the identities of the victims are still unclear. And while the Chinese deployed the attack widely, they might have sought only to take information from a narrow group of targets in which they have the highest interest.

There is little doubt that the scope of the attack has American officials considering whether they will have to retaliate against China as well. That would put them in the position of engaging in a potentially escalating conflict with two countries that are also its biggest nuclear-armed adversaries.

It has become increasingly clear in recent days that the hacking that Microsoft has attributed to Beijing poses many of the same challenges as the SolarWinds attack conducted by the Russians, although the targets and the methodology are significantly different.

Like the Russians, the Chinese attackers initiated their campaign against Microsoft from computer servers — essentially cloud services — that they rented under assumed identities in the United States. Both countries know that American law prohibits intelligence agencies from looking in systems based in the United States, and they are exploiting that legal restriction.

“The Chinese actor apparently spent the time to research the legal authorities and recognized that if they could operate from inside the United States, it takes some of the government’s best threat-hunters off the field,” Tom Burt, the Microsoft executive overseeing the investigation, said on Friday.

The result was that in both the SolarWinds and the more recent Chinese hacking, American intelligence agencies appeared to have missed the evidence of what was happening until a private company saw it and alerted the authorities.

The debate preoccupying the White House is how to respond. Mr. Sullivan served as Mr. Biden’s national security adviser while he was vice president, as the Obama administration struggled to respond to a series of attacks.

Those included the Chinese effort that stole 22.5 million security-clearance records from the Office of Personnel Management in 2014 and the Russian attack on the 2016 presidential election.

In writings and talks over the past four years, Mr. Sullivan has made clear that he believes traditional sanctions alone do not sufficiently raise the cost to force powers like Russia or China to begin to talk about new rules of the road for cyberspace.

But government officials often fear that too strong a response risks escalation.

That is a particular concern in the Russian and Chinese attacks, where both countries have clearly planted “back doors” to American systems that could be used for more destructive purposes.

American officials say publicly that the current evidence suggests that the Russian intention in the SolarWinds attack was merely data theft. But several senior officials, when speaking not for attribution, said they believed the size, scope and expense of the operation suggested that the Russians might have had much broader motives.

“I’m struck by how many of these attacks undercut trust in our systems,” Mr. Burt said, “just as there are efforts to make the country distrust the voting infrastructure, which is a core component of our democracy.”

Russia broke into the Democratic National Committee and state voter-registration systems in 2016 largely by guessing or obtaining passwords. But they used a far more sophisticated method in the SolarWinds hacking, inserting code into the company's software updates, which ushered them deep into about 18,000 systems that used the network management software. Once inside, the Russians had high-level access to the systems, with no passwords required.

Similarly, four years ago, a vast majority of Chinese government hacking was conducted via email spear-phishing campaigns. But over the past few years, China's military hacking divisions have been consolidating into a new strategic support force, similar to the Pentagon's Cyber Command. Some of the most important hacking operations are run by the stealthier Ministry of State Security, China's premier intelligence agency, which maintains a satellite network of contractors.

Beijing also started hoarding so-called zero-days, flaws in code unknown to software vendors and for which a patch does not exist.

In August 2019, security researchers got their first glimpse of how these undisclosed zero-day flaws were being used: Security researchers at Google's Project Zero and Volexity — the same company in Reston, Va., that discovered the Microsoft attack — found that Chinese hackers were using a software vulnerability to spy on anyone who visited a website read by Uighurs, an ethnic minority group whose persecution has drawn international condemnation.

For two years, until the campaign was discovered, anyone who visited the sites unwittingly downloaded Chinese implants onto their smartphones, allowing Beijing to monitor their communications.

Kevin Mandia of FireEye, Sudhakar Ramakrishna of SolarWinds and Brad Smith of Microsoft testified last month in a Senate Intelligence Committee hearing on the Russian hacking.Credit...Drew Angerer/Agence France-Presse, via Pool/Afp Via Getty Images

The Chinese attack on Microsoft’s servers used four zero-days flaws in the email software. Security experts estimated on Friday that as many as 30,000 organizations were affected by the hacking, a detail first reported by the security writer Brian Krebs. But there is some evidence that the number could be much higher.