How China’s Devastating Microsoft Hack Puts Us All at Risk

thedailybeast.com/how-chinas-devastating-microsoft-hack-puts-us-all-at-risk

SpyTalk March 15, 2021

Tech

DEEP STRIKE

The new battlefield, with its potential for attacks on power grids, hospitals, and sensitive facilities like nuclear power plants, puts entire populations in significant danger.

Michael Borgers/Getty

By Matthew Brazil

During World War II, the Chinese communists cultivated opium in their base area and trafficked it into Japanese-occupied cities. Mao Zedong’s man in charge was one of the biggest master spies of the period, Li Kenong. Though Mao later regretted cultivating the “special product,” which he called “that certain thing,” the drug caused disruption in the enemy rear and benefited the Red-area economy.

Now it seems to be applying the same strategy in the West’s rear area, causing disruptions to online systems and simultaneously benefiting the Chinese economy with viruses and worms used to steal information from computer systems worldwide. The latest simultaneous

exploit against thousands of organizations, disclosed on March 2, was dubbed the Microsoft Exchange hack, exploiting servers that manage email systems. The hack allows perpetrators to read messages of selected targets and then venture deeper into infected networks.

Over 60,000 organizations in the U.S. and at least 280,000 users worldwide using Microsoft Exchange for their email were hacked between Feb. 26 and March 3, according to Chris Krebs, the former director of the Cybersecurity and Infrastructure Security Agency. The organizations include defense contractors, universities, state and local governments, policy think tanks, infectious disease researchers, and businesses: anyone that chose to use Microsoft Exchange for their email service.

The unidentified organization behind the hack, assessed by Microsoft to be a Chinese state-sponsored entity, is known by the code name HAFNIUM. The hack has enabled unauthorized access to entire email systems and follow-on access to connected databases that store classified information, trade secrets, the wide range of other proprietary information, and personally identifiable information such as names, addresses, Social Security numbers, and so on that is useful for identity theft.

Named after a chemical element discovered in 1923, HAFNIUM is a new activity and not yet clearly identified to the point where it would receive a cryptonym such as "TURBINE PANDA"—the name given to the cyber espionage activities at the infamous Jiangsu State Security Bureau.

TURBINE PANDA is linked to the 2014 OPM hack, another massive data breach, and to the case of Yanjun Xu, the State Security officer extradited to the U.S. from Belgium for attempted theft of GE advanced jet engine technology.

Bad actors in China and beyond, whether working on behalf of intelligence services or criminal organizations**,** are expected to rapidly develop HAFNIUM "proof of concept exploits," i.e. to show that they can use the vulnerability to burrow into a target system by performing benign tasks like opening up the calculator, or moving the cursor. From there, it is a short step to weaponizing the exploit with malware.

According to an industry source, several other Chinese hacking groups may have used the same zero-day vulnerabilities as did HAFNIUM. Criminal organizations outside China have already employed ransomware using the vulnerability a mere nine days after it was discovered, faster than in previous cases.

That will further challenge cybersecurity detectives in their attempts to attribute the attacks to specific entities.

The situation is so toxic that the Biden administration issued a public warning on March 12 that organizations "have hours, not days" to update exposed servers with software patches already issued by Microsoft. Ordinary users may have noticed two long updates from Microsoft in the past week that are intended to eliminate vulnerabilities.

That Microsoft has identified HAFNIUM as a Chinese state-sponsored actor indicates that Beijing's security services, likely the Ministry of State Security (MSS), continue to pursue the massive harvesting of data such as the 2017 APT 3 exploit, attributed to the Guangdong State Security Bureau.

It is no surprise that the multi-stage, malicious HAFNIUM operation from China against Microsoft Exchange servers bears some operational resemblance to the SolarWinds attack from Russia. Both rely on widespread use of a targeted system, i.e. Solar Winds and Microsoft Exchange, as the vector to reach the real objective: the tens of thousands of users who possess sensitive information like U.S. defense production data, weapons systems designs, trade secrets useful to China's latest Five-Year Plan, and the emails of Beijing's perceived political enemies.

These intelligence objectives are reminiscent of the targets of Russian and Chinese communist intelligence agencies over the past century. From the late 1920s until the late 1950s, the spy services of Russia and communist China shared selected information about their common enemies: Japan and Germany in World War II, the U.S. and its allies early in the Cold War.

It remains to be seen if evidence emerges of modern-day cooperation between Moscow and Beijing, whose relations have steadily improved since the collapse of the Soviet Union in 1991, to research and carry out cyber attacks. Although it is a tenuous link, evidence emerged on March 8 that hackers from China targeted SolarWinds customers in an operation that was distinct from the related Russian attacks.

These exploits underline how large scale computer network exploitation in the 21st century has reshaped technical intelligence collection, and not just among the superpowers. During the Cold War, useful signal intelligence operations required the resources of an advanced industrial state. Now the advantage in conducting massive, devastating hacks belongs to whatever player, large or small, has the best software developers.

The new battlefield, with its potential for attacks on power grids, hospitals, and sensitive facilities like nuclear power plants, puts entire populations in significant danger.

Although individual users may feel helpless in this *Black Mirror*-type scenario, they have within their grasp several easy fixes that anyone, technical or not, can employ.

The first step is to enable two-factor authentication in application launches whenever possible. This makes it difficult for a third party to intrude into your account if they have managed to steal your password.

Second, and the most common and yet commonly ignored advisory: Don't ever click on links in emails unless you are certain that they are legitimate. That's how adversaries have gained entrance to Pentagon computers again and again.

Just. Don't. Click. Unless you want to end up like Hillary Clinton's campaign chairman John Podesta, with your emails hacked and shared with the world.

Third, users exchanging sensitive information especially should employ a virtual private network (VPN) to hide their traffic. In this day and age, why not obscure every keystroke and web search from prying eyes?

Fourth, never put off software updates. There is a big market internationally not only for zero-day vulnerabilities, but also for one-day (publicly known and patched) vulnerabilities. Why? A high percentage of users skip updates, leaving themselves open to well-known exploits already publicly shared worldwide on Github, the open, cloud-based software sharing service,

Once an exploit is posted on Github, anyone can use it. Criminals then go after low hanging fruit, including the vast number of people who don't bother with software updates and patches. That especially includes those using pirated software. Previously a cheap alternative, pirated software has become the Typhoid Mary of the digital space.

Need some motivation to do the right things? Take a look at *This Is How They Tell Me the World Ends*, a scary exposé of the worldwide cyber weapons market that is partly fueled by American taxpayer dollars. China is certainly watching.

Co-published with SpyTalk*, where Jeff Stein leads an all-star team of veteran investigative reporters, writers, and subject-matter experts who will take you behind the scenes of the national security state. Subscribe to get full access to the newsletter and website.*