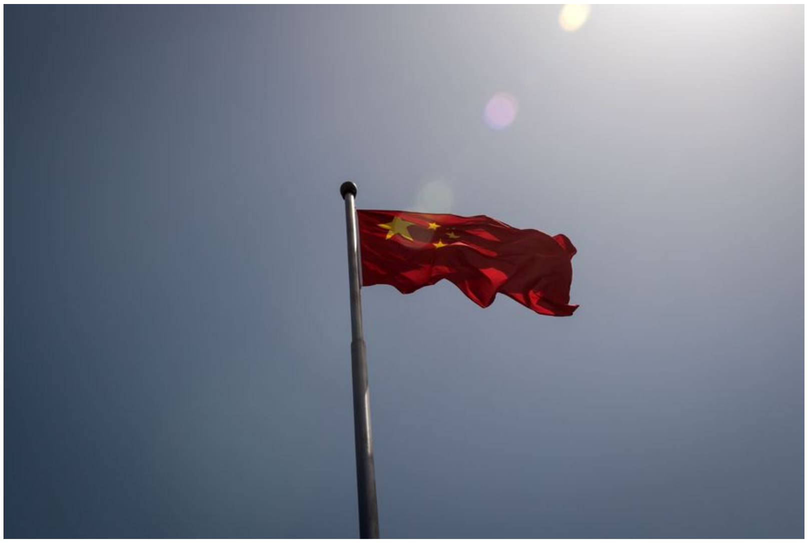
https://www.wsj.com/articles/wave-of-stealthy-china-cyberattacks-hits-u-s-private-networks-google-says-2f98eaed

◆ WSJ NEWS EXCLUSIVENATIONAL SECURITY

Wave of Stealthy China Cyberattacks Hits U.S., Private Networks, Google Says

Attacks represent new level of ingenuity and sophistication from China, according to researchers



China has routinely denied hacking into businesses or governments in other countries.

PHOTO: NICOLAS ASFOURI/AGENCE FRANCE-PRESSE/GETTY IMAGES

By Robert McMillan Follow *in San Francisco and Dustin Volz* Follow *in Washington*

Updated March 16, 2023 12:12 pm ET

State-sponsored hackers from China have developed techniques that evade common cybersecurity tools and enable them to burrow into government and business networks and spy on victims for years without detection, researchers with Alphabet Inc.'s Google found.

Over the past year, analysts at Google's Mandiant division have discovered hacks of systems that aren't typically the targets of cyber espionage. Instead of infiltrating systems behind the corporate firewall, they are compromising devices on the edge of the network—sometimes firewalls themselves—and targeting software built by companies such as VMware Inc. or Citrix Systems Inc. These products run on computers that don't typically include antivirus or endpoint detection software.

The attacks routinely exploit previously undiscovered flaws and represent a new level of ingenuity and sophistication from China, said Charles Carmakal, Mandiant's chief technology officer. Researchers have linked the activity to a suspected China-nexus hacking group because of the profile of victims, including some who have been hit repeatedly, the high degree of novel tradecraft and sophistication observed and level of resources required, and the identification of obscure malware code only known to have been used by China-based threat actors in the past, among other reasons.

China has routinely denied hacking into businesses or governments in other countries and accused the U.S. and its allies of the practice. The Chinese Embassy in Washington didn't immediately respond to a request for comment.

With the exception of a widespread 2021 attack on servers running Microsoft's Exchange email software that was linked to China, China's attacks have been precisely aimed, often hitting only a handful of high-value government and business victims, Mr. Carmakal said. The tactics deployed are so stealthy that Mandiant believes the scope of Chinese intrusion into U.S. and Western targets is likely far broader than currently known, he said.

The method of cyberattack "is a lot harder for us to investigate, and it is certainly exponentially harder for victims to discover these intrusions on their own," Mr. Carmakal said. "Even with our hunting techniques, it's hard for them to find it."

Senior U.S. officials have long viewed Beijing as a top cyber-espionage threat.

PHOTO: NOEL CELIS/AGENCE FRANCE-PRESSE/GETTY IMAGES

The findings shared Thursday come amid heightened concerns about the breadth of Chinese espionage against the West following last month's discovery of an alleged Chinese surveillance balloon that invaded U.S. airspace and a bipartisan push in Washington to ban the social-media app TikTok due to data security fears.

Defense contractors, government agencies, and technology and telecommunications firms appeared to be bearing the brunt of the newly discovered Beijing-linked attacks, Mr. Carmakal said. While the relative quantity of identified victims may be small—perhaps in the dozens—the impact is significant because of the importance of what is being stolen, he said.

Senior U.S. officials have long viewed Beijing as a top cyber-espionage threat and have for years been alarmed at the success Chinese hacking groups have had in compromising military targets and defense contractors to steal advanced military technology. U.S. intelligence agencies have similarly observed improving tradecraft from hackers suspected of working on behalf of the Chinese Communist Party. In an annual worldwide threat assessment published earlier this month, U.S. intelligence officials said China "probably currently represents the broadest, most active, and persistent cyber espionage threat to U.S. government and private-sector networks."

In the recently discovered series of hacks, often the systems breached were the very ones designed to protect companies.

In January, for example, Mandiant warned of an attack linked to China targeting a bug in firewall software built by the security firm Fortinet Inc. And on Thursday, Mandiant said that it had jointly discovered a second Fortinet bug, which was patched last week, that was also being exploited by China-linked hackers.

A Fortinet spokeswoman said that the company had patched the bug disclosed in March, and that the company wouldn't speculate on who was behind the attack. According to the company's website, the bug disclosed in January has also been patched. In an analysis, published by Fortinet, the company said that the complexity of the January attack "suggests an advanced actor."

In another attack, the hackers linked to China exploited a previously patched bug in mobile access software built by the firm SonicWall Inc. But they also developed a system that would allow them to retain access to the device, even when its software was updated, an unusual technique that reflected the amount of effort the hackers were willing to spend in the attack, Mandiant said.

“There is a lot of intrusion activity going undetected,” Mr. Carmakal said. “We think the problem is a lot bigger than we know today.”

SonicWall has since released new firmware that would prevent this technique from working, and the bug exploited by the attackers was patched in 2021, a SonicWall spokesman said.

In December, the National Security Agency took the unusual step of warning U.S. organizations that a China-linked hacking group known as APT5 had been targeting Citrix’s software.

Citrix didn’t respond to messages seeking comment. A VMware spokeswoman said that the company had issued instructions on how customers could improve security on its virtual machine software.

Write to Robert McMillan at robert.mcmillan@wsj.com and Dustin Volz at dustin.volz@wsj.com