Written by **Luis Miguel** on March 19, 2023

Researchers: China Getting Better at Hiding Cyberspying

ilkaydede/iStock/Getty Images Plus

In China's campaign of unrestricted warfare against the United States, espionage is one of the most important components powering Beijing's ability to outmaneuver America on every relevant front. And, unfortunately for the U.S., it appears China is only getting better at its ability to spy without detection.

This is the alarm being rung by researchers at the Google-owned cybersecurity firm Mandiant. According to the researchers, hacking groups with suspected ties to China have developed new methods for breaking through internet-facing security tools in order to discreetly get into the databases of data-rich organizations.

The researchers shared their findings in a Thursday report in which they asserted that they unearthed a bug that was targeting Fortinet, the software security company known for making an assortment of tools, from firewalls to antivirus programs.

The two malware strains identified by Mandiant, CastleTap and ThinCrust, went after vulnerabilities in Fortinet for the purpose of accessing data from companies working in the defense, telecom, and government contracting spheres.

The report describes that, in one instance, hackers slipped bad code onto the security tool known as FortiManager while it was linked to the internet. By means of that code, the hackers were able to easily install malware and access other products connected to the same network.

Through this method of targeting internet-facing security tools, bad actors can break their way into a network without human interaction. Traditional malware processes require that users install a corrupted program or install a phishing link in order to give the hacker access.

What this does is make the cyberattacks harder to detect, providing hackers with more time to steal data.

The Mandiant report concluded:

> The activity discussed in this blog post is further evidence that advanced cyber espionage threat actors are taking advantage of any technology available to persist and traverse a target environment, especially those technologies that do not support EDR solutions. This presents a unique challenge for investigators as many network appliances lack solutions to detect runtime modifications made to the underlying operating system and require direct involvement of the manufacturer to collect forensic images. Cross organizational communication and collaboration is key to providing both manufacturers with early notice of new attack methods in the wild before they are made public and investigators with expertise to better shed light on these new attacks.

The report is the fifth detailing attacks by suspected Chinese hackers that Mandiant has published in the last two years alone. In the past, companies that have been targeted by malicious actors were SonicWall, VMware, and Citrix.

Fears of Chinese surveillance of America's government and people have been high in recent days, particularly after a Chinese-operated high-altitude spy balloon was spotted flying over the United States. The Biden administration finally had the balloon shot down — after a week of letting it hover over the country.

Now the White House is pushing for something the Trump administration attempted: Banning TikTok, the popular video-based social media app owned by Chinese tech company ByteDance.

The Committee on Foreign Investment (CFIUS) has given ByteDance an ultimatum: Sell TikTok or the app will be banned in the United States.

In a final bid to avoid a sale and prevent a ban, TikTok has recruited dozens of content creators with significant followings on the app to participate in a Wednesday press conference in Washington, D.C. The company is paying for these influencers' travel expenses in the hope that this will convince policymakers to desist from the crackdown.

In some ways, the U.S. government is making spying easier for China. TP-Link, one of the world's top manufacturers of internet routers and other electronic devices, has been used on American military bases and purchased in large quantities by the Defense Department despite being a China-based firm that not only collects personal data through its products, but openly admits that any user's personal information can be shared through TP-Link's network.

In its 2023 worldwide threats report, the U.S. intelligence community said this month that Beijing is the "broadest, most active and persistent" cyberspying threat to America.

The report further reads:

> China almost certainly is capable of launching cyber attacks that could disrupt critical infrastructure services within the United States, including against oil and gas pipelines, and rail systems.
>
> … China's cyber espionage operations have included compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations.

The intelligence community contends that China targets journalists, dissidents, and those it views as threats, often with the aim of countering views the CCP considers critical of China.

As *The New American* has reported, China is in the process of widening its global sphere of influence, building strategic partnerships on every continent.

Recent Chinese incursions in Latin America should be cause for major concern. At a rapid rate, China is leaving the United States behind, outpacing America in terms of global support, military prowess, economic relevance, and technological capabilities.