

China Hijacked an NSA Hacking Tool in 2014—and Used It for Years

Andy Greenberg : 8-10 minutes : 2/22/2021

More than four years after a [mysterious group of hackers known as the Shadow Brokers](#) began wantonly [leaking secret NSA hacking tools](#) onto the internet, the question that debacle raised—whether any intelligence agency can prevent its "zero-day" stockpile from [falling into the wrong hands](#)—still haunts the security community. That wound has now been reopened, with evidence that Chinese hackers obtained and reused another NSA hacking tool years before the Shadow Brokers brought it to light.

On Monday, the security firm Check Point revealed that it had discovered evidence that a Chinese group known as APT31, also known as Zirconium or Judgment Panda, had somehow gained access to and used a Windows-hacking tool known as EpMe created by the Equation Group, a security industry name for the highly sophisticated hackers widely understood to be a part of the NSA. According to Check Point, the Chinese group in 2014 built their own hacking tool from EpMe code that dated back to 2013. The Chinese hackers then used that tool, which Check Point has named "Jian" or "double-edged sword," from 2015 until March 2017, when Microsoft patched the vulnerability it attacked. That would mean APT31 had access to the tool, a "privilege escalation" exploit that would allow a hacker who already had a foothold in a victim network to gain deeper access, long before the late 2016 and early 2017 Shadow Brokers leaks.

Only in early 2017 did Lockheed Martin discover China's use of the hacking technique. Because Lockheed has largely US customers, Check Point speculates that the hijacked hacking tool may have been used against Americans. "We found conclusive evidence that one of the exploits that the Shadow Brokers leaked had somehow already gotten into the hands of Chinese actors," says Check Point's head of cyber research Yaniv Balmas. "And it not only got into their hands, but they repurposed it and used it, likely against US targets."

A source familiar with Lockheed Martin's cybersecurity research and reporting confirms to WIRED that the company found the Chinese hacking tool being used in a US private sector network—not its own or part of its supply chain—that was not part of the US defense industrial base, but declined to share more details. An email from a Lockheed Martin spokesperson responding to Check Point's research states only that the company's "cybersecurity team routinely evaluates third-party software and technologies to identify vulnerabilities and responsibly report them to developers and other interested parties."

Check Point's findings aren't the first time that Chinese hackers have reportedly repurposed an NSA hacking tool—or at least, an NSA hacking technique. [Symantec in 2018 reported that another powerful Windows zero-day vulnerability](#), exploited in the NSA hacking tools EternalBlue and EternalRomance, had also been repurposed by Chinese hackers prior to their disastrous exposure by the Shadow Brokers. But in that case, Symantec noted that it didn't seem that the Chinese hackers actually gained access to the NSA's malware. Instead, it appeared they had seen the agency's network communications and reverse engineered the techniques it used to build their own hacking tool.

APT31's Jian tool, by contrast, appears to have been built by someone with hands-on access to the Equation Group's compiled program, Check Point's researchers say, in some cases duplicating arbitrary or nonfunctional parts of its code. "The Chinese exploit copied some part of the code, and in some cases they seem like they didn't really understand what they copied and what it does," says Check Point researcher Itay Cohen.

While Check Point states with certainty that the Chinese group took its Jian hacking tool from the NSA, there's some room for debate as to its origins, says Jake Williams, the founder of Rendition Infosec and a former NSA hacker. He points out that Check Point reconstructed that code's history by looking at compile times, which could be faked. There could even be a missing, earlier sample that shows the tool originated with the Chinese hackers and was taken by the NSA, or even that it started with a third hacker group. "I think they have a field-of-view bias by saying this was *definitely* stolen from NSA," Williams says. "But for whatever it's worth, if you forced me to put money on who had it first, I'd say NSA."

Check Point says it doesn't know how the APT31 hackers, who most recently came into the spotlight last October when [Google reported they had targeted the campaign of then presidential candidate Joe Biden](#), would have laid hands on the NSA hacking tool. They speculate that the Chinese hackers might have grabbed the EpMe malware from a Chinese network where Equation Group had used it, from a third-party server where Equation Group had stored it to be used against targets without revealing their origin, or even from the Equation Group's own network—in other words, from inside the NSA itself.

The researchers say they made their discovery while digging through older Windows privilege escalation tools to create "fingerprints" that they could use to attribute those tools to certain groups. The approach helps better identify the origin of hackers found inside customers' networks. At one point Check Point tested one of these fingerprints its researchers had created from the APT31 hacking tool and were surprised to find that it matched not Chinese code, but Equation Group tools from the Shadow Brokers' leak. "When we got the results, we were in shock," says Cohen. "We saw that this was not only the same exploit, but when we analyzed the binary we found that the Chinese version is a replica of the Equation Group exploit from 2013."




That discovery led Check Point to more closely examine the group of tools in which EpMe was found in the Shadow Brokers' data dump. That group included three other exploits, two of which had used vulnerabilities discovered by Russian security firm Kaspersky that were patched by Microsoft prior to the Shadow Brokers' release. They also noted another exploit called EpMo that has received little public discussion and was silently patched by Microsoft in May 2017, after the Shadow Brokers' leak.

When WIRED reached out to Microsoft, a spokesperson responded in a statement: "We confirmed in 2017 that the exploits disclosed by Shadow Brokers have already been addressed. Customers with up-to-date software are already protected against the vulnerabilities mentioned in this research."

As Check Point's "double-edged sword" name for the Chinese version of the repurposed NSA malware implies, the researchers argue their findings should raise again the question of whether intelligence agencies can safely hold and use zero-day hacking tools without risking that they lose control of them. "This is exactly the definition of a double-edged sword," says Balmas. "Maybe the hand is too quick on the trigger. Maybe you should patch quicker. Nations will always have zero days. But perhaps the way we handle them ... we might need to think about this again."

Update 12:20pm EST: *This story has been updated with a statement from Lockheed Martin.*
Updated 1:10pm EST: *This story has been updated again with additional details from a source familiar with Lockheed Martin's cybersecurity research and reporting.*

More Great WIRED Stories

-  The latest on tech, science, and more: [Get our newsletters!](#)
- Premature babies and the [lonely terror of a pandemic NICU](#)
- Researchers levitated a small tray [using nothing but light](#)
- The recession exposes the US' [failures on worker retraining](#)
- Why insider "Zoom bombs" [are so hard to stop](#)
- How to [free up space on your laptop](#)
-  WIRED Games: Get the latest [tips, reviews, and more](#)
-  Want the best tools to get healthy? Check out our Gear team's picks for the [best fitness trackers](#), [running gear](#) (including [shoes](#) and [socks](#)), and [best headphones](#)