The Mystery of ‘Jia Tan,’ the XZ Backdoor Mastermind

Andy Greenberg, Matt Burgess ⋮ 4-5 minutes ⋮ 4/3/2024

Ultimately, Scott argues that those three years of code changes and polite emails were likely not spent sabotaging multiple software projects, but rather building up a history of credibility in preparation for the sabotage of XZ Utils specifically—and potentially other projects in the future. “He just never got to that step because we got lucky and found his stuff,” says Scott. “So that’s burned now, and he’s gonna have to go back to square one.”

Technical Ticks and Time Zones

Despite Jia Tan’s persona as a single individual, their yearslong preparation is a hallmark of a well-organized state-sponsored hacker group, argues Raiu, the former Kaspersky lead researcher. So too are the technical hallmarks of the XZ Utils malicious code that Jia Tan added. Raiu notes that, at a glance, the code truly looks like a compression tool. “It’s written in a very subversive manner,” he says. It’s also a “passive” backdoor, Raiu says, so it wouldn’t reach out to a command-and-control server that might help identify the backdoor’s operator. Instead, it waits for the operator to connect to the target machine via SSH and authenticate with a private key—one generated with a particularly strong cryptographic function known as ED448.

The backdoor’s careful design could be the work of US hackers, Raiu notes, but he suggests that’s unlikely, since the US wouldn’t typically sabotage open source projects—and if it did, the National Security Agency would probably use a quantum-resistant cryptographic function, which ED448 is not. That leaves non-US groups with a history of supply chain attacks, Raiu suggests, like China’s APT41, North Korea’s Lazarus Group, and Russia’s APT29.

At a glance, Jia Tan certainly looks East Asian—or is meant to. The time zone of Jia Tan’s commits are UTC+8: That’s China’s time zone, and only an hour off from North Korea’s. However, an analysis by two researchers, Rhea Karty and Simon Henniger, suggests that Jia Tan may have simply changed the time zone of their computer to UTC+8 before every commit. In fact, several commits were made with a computer set to an Eastern European or Middle Eastern time zone instead, perhaps when Jia Tan forgot to make the change.

“Another indication that they are not from China is the fact that they worked on notable Chinese holidays,” say Karty and Henniger, students at Dartmouth College and the Technical University of Munich, respectively. They note that Jia Tan also didn't submit new code on Christmas or New Year's. Boehs, the developer, adds that much of the work starts at 9 am and ends at 5 pm for Eastern European or Middle Eastern time zones. “The time range of commits suggests this was not some project that they did outside of work,” Boehs says.

Though that leaves countries like Iran and Israel as possibilities, the majority of clues lead back to Russia, and specifically Russia’s APT29 hacking group, argues Dave Aitel, a former NSA hacker and founder of the cybersecurity firm Immunity. Aitel points out that APT29—widely believed to work for Russia’s foreign intelligence agency, known as the SVR—has a reputation for technical care of a kind that few other hacker groups show. APT29 also carried out the Solar Winds compromise, perhaps the most deftly coordinated and effective software supply chain attack in history. That operation matches the style of the XZ Utils backdoor far more than the cruder supply chain attacks of APT41 or Lazarus, by comparison.

“It could very well be someone else,” says Aitel. “But I mean, if you’re looking for the most sophisticated supply chain attacks on the planet, that’s going to be our dear friends at the SVR.”

Security researchers agree, at least, that it’s unlikely that Jia Tan is a real person, or even one person working alone. Instead, it seems clear that the persona was the online embodiment of a new tactic from a well-organized group—a tactic that nearly worked. That means we should expect to see Jia Tan return by other names: seemingly polite and enthusiastic contributors to open source projects, hiding a government’s secret intentions in their code commits.

Updated 4/3/2024 at 12:30 pm ET to note the possibility of Israeli or Iranian involvement.