5 takeaways from Twitter whistleblower Peiter Zatko

August 24 2022, by DAVID HAMILTON

The logo for Twitter appears above a trading post on the floor of the New York Stock Exchange, Nov. 29, 2021. Startling new revelations from Twitter's former head of security, Peiter Zatko, have raised serious new questions about the security of the platform's service, its ability to identify and remove fake accounts, and the truthfulness of its statements to users, shareholders and federal regulators. Credit: AP Photo/Richard Drew, File

Startling new revelations from Twitter's former head of security, Peiter Zatko, have raised serious new questions about the security of the platform's service, its ability to identify and remove fake accounts, and the truthfulness of its statements to users, shareholders and federal regulators.

Zatko—better known by his hacker handle "Mudge"—is a respected cybersecurity expert who first gained prominence in the 1990s and later worked in senior positions at the Pentagon's Defense Advanced Research Agency and Google. Twitter fired him from the security job early this year for what the company called "ineffective leadership and poor performance." Zatko's attorneys say that claim is false.

In a whistleblower complaint made public Tuesday, Zatko documented what he described as his uphill 14-month effort to bolster Twitter security, boost the reliability of its service, repel intrusions by agents of foreign governments and both measure and take action against fake "bot" accounts that spammed the platform.

Many of Zatko's claims have not been corroborated and the complaint did not provide documentary support for them. In a statement, Twitter called Zatko's description of events "a false narrative."

Here are five takeaways from that whistleblower complaint.

TWITTER'S SECURITY AND PRIVACY SYSTEMS WERE GROSSLY INADEQUATE

In 2011, Twitter settled a Federal Trade Commission investigation into its privacy practices by agreeing to put stronger data security protections in place. Zatko's complaint charges that Twitter's problems grew worse over time instead.

For instance, the complaint states, Twitter's internal systems allowed far too many employees access to personal user data they didn't need for their jobs—a situation ripe for abuse. For years, Twitter also continued to mine user data such as phone numbers and email addresses—intended only for security purposes—for ad targeting and marketing campaigns, according to the complaint.

TWITTER'S ENTIRE SERVICE COULD HAVE COLLAPSED IRREPARABLY UNDER STRESS

One of the most striking revelations in Zatko's complaint is the claim that Twitter's internal data systems were so ramshackle—and the company's contingency plans so insufficient—that any widespread crash or unplanned shutdown could have tanked the entire platform.

The concern was that a "cascading" data-center failure could quickly spread across Twitter's fragile information systems. As the complaint put it: "That meant that if all the centers went offline simultaneously, even briefly, Twitter was unsure if they could bring the service back up. Downtime estimates ranged from weeks of round-the-clock work, to permanent irreparable failure."

TWITTER MISLED REGULATORS, INVESTORS AND MUSK ABOUT FAKE "SPAM" BOTS

In essence, Zatko's complaint states that Tesla CEO Elon Musk—whose $44 billion bid to acquire Twitter is headed for October trial in a Delaware court—is correct when he charges that Twitter executives have little incentive to accurately measure the prevalence of fake accounts on the system.

The complaint charges that the company's executive leadership practiced "deliberate ignorance" on the subject of these so-called spam bots.

"Senior management had no appetite to properly measure the prevalence of bot accounts," the complaint states, adding that executives were concerned that accurate bot measurements would harm Twitter's "image and valuation."

ON JAN. 6, 2021, TWITTER COULD HAVE BEEN AT THE MERCY OF DISGRUNTLED EMPLOYEES

Zatko's complaint states that as a mob assembled in front of the U.S. Capitol on Jan. 6, 2021, eventually storming the building, he began to worry that employees sympathetic to the rioters might try to sabotage Twitter. That concern spiked when he learned it was "impossible" to protect the platform's core systems from a hypothetical rogue or disgruntled engineer aiming to wreak havoc.

"There were no logs, nobody knew where data lived or whether it was critical, and all engineers had some form of critical access" to Twitter's core functions, the complaint states.

A PLAYGROUND FOR FOREIGN GOVERNMENTS

The Zatko complaint also highlights Twitter's difficulty in identifying—much less resisting—the presence of foreign agents on its service. In one instance, the complaint alleges, the Indian government required Twitter to hire specific individuals alleged to be spies, and who would have had significant access to sensitive data thanks to Twitter's own lax security controls. The complaint also alleges a murkier situation involving taking money from unidentified "Chinese entities" that then could access data that might endanger Twitter users in China.