On Wednesday, July 15, 2020, Twitter detected a security incident and took immediate action.

The attack targeted certain Twitter employees through social engineering. The attackers successfully manipulated a small number of employees and used their credentials to access Twitter's internal systems, including getting through our two-factor protections. For 45 of those accounts, the attackers were able to initiate a password reset, login to the account, and send Tweets. In addition, they may have attempted to sell some of the usernames.

What the attackers accessed

The most important question for people who use Twitter is likely — did the attackers see any of my private information? For the vast majority of people, we believe the answer is, no. For the 130 accounts that were targeted, here is what we know as of today.

- Attackers were not able to view previous account passwords, as those are not stored in plain text or available through the tools used in the attack.
- Attackers were able to view personal information including email addresses and phone numbers, which are displayed to some users of our internal support tools.
- In cases where an account was taken over by the attacker, they may have been able to view additional information.

The forensic investigation of these activities is still ongoing.

Twitter is actively working on communicating directly with the account-holders that were impacted. – Twitter's response.

What does this mean to RAVENii Clients?

Because of the limited scope of this attack, the likelihood that an employee of our customers is at risk is slim. We are not recommending drastic measures, such as removing access to this application. In some roles, this application is a vital tool for research and user group information. However, we would suggest that this is a great reminder to focus on your access management controls. Ensure that employees with elevated access to systems are aware of the incident. Take this time to ensure that all employees have minimum necessary access to systems based on their job function. We would also suggest that employees that use Twitter, immediately change their password. A reminder that frequently changing passwords and implementing strong passwords standards is a key step in thwarting the adversaries. This would be a good time to provide some basic end-user security training around passwords and phishing tactics.

At this point there is no reason to believe that there are tangential risks to the Twitter breach. However, if an employee is contacted by Twitter they should immediately notify management and the RAVENii Security Operation Center or Virtual Chief Information Security Officer to evaluate risk. RAVENii will continue to monitor the situation and keep our clients informed.