A teen is reportedly the mastermind behind the Lapsus$ hacking group

In recent weeks, the Lapsus$ hacking group has taken credit for accessing company data from Nvidia, Samsung, Ubisoft, Okta, and even Microsoft, and according to a new *Bloomberg* report, an England-based teenager might be the person heading up the operation.

“Four researchers investigating the hacking group Lapsus$, on behalf of companies that were attacked, said they believe the teenager is the mastermind,” *Bloomberg* said. However, the teenager, who apparently uses the online aliases “White” and “breachbase,” has not been accused by law enforcement, and the researchers “haven’t been able to conclusively tie him to every hack Lapsus$ has claimed,” *Bloomberg* said.

The teenager is apparently based about five miles outside of Oxford University, and *Bloomberg* says it was able to speak to his mother for ten minutes through a “doorbell intercom system” at the home. The teenager’s mother told the publication she did not know of allegations against him. “She declined to discuss her son in any way or make him available for an interview, and said the issue was a matter for law enforcement and that she was contacting the police,” *Bloomberg* said.

Lapsus$ apparently doesn’t just consist of the England-based teenager, though. *Bloomberg* reports that one suspected member is another teenager in Brazil and that seven unique accounts have been linked with the group. One of the members is apparently such a capable hacker that researchers thought the

work was automated, one person involved in research about the group told *Bloomberg*.

According to cybersecurity expert Brian Krebs, a core member of Lapsus$, who may have used the aliases “Oklaqq” and “WhiteDoxbin,” also purchased Doxbin, a website where people can post or search for the personal information of others for the purposes of doxing. This WhiteDoxbin individual apparently wasn’t the best admin and had to sell the site back to its previous owner, but leaked “the entire Doxbin data set,” which led to the Doxbin community *doxing WhiteDoxbin*, “including videos supposedly shot at night outside his home in the United Kingdom,” Krebs reported.

Krebs also reports that this person may have been behind the EA data breach that took place last year. What may connect the person between *Bloomberg* and Krebs’ is the name “breachbase.”

From Krebs:

> *Back in May 2021, WhiteDoxbin’s Telegram ID was used to create an account on a Telegram-based service for launching distributed denial-of-service (DDoS) attacks, where they introduced themself as “@**breachbase**.” News of EA’s hack last year was first posted to the cybercriminal underground by the user “Breachbase” on the English-language hacker community **RaidForums**, which was recently seized by the FBI.*

The full picture surrounding Lapsus$ is still murky, but I strongly urge you to read both *Bloomberg* and Krebs’ reports to learn more about what may be going on.

https://www.theverge.com/2022/3/23/22993731/lapsus-hacking-group-teenager-mastermind