Microsoft says early June disruptions to Outlook, cloud platform, were cyberattacks

June 18 2023, by Frank Bajak

The Microsoft company logo is displayed at their offices in Sydney, Australia, on Feb. 3, 2021. Microsoft says the early June 2023 disruptions to its Microsoft's flagship office suite — including the Outlook email and OneDrive file-sharing apps — were denial-of-service attacks by a shadowy new hacktivist group. Credit: AP Photo/Rick Rycroft, File

In early June, sporadic but serious service disruptions plagued

Microsoft's flagship office suite—including the Outlook email and OneDrive file-sharing apps—and cloud computing platform. A shadowy hacktivist group claimed responsibility, saying it flooded the sites with junk traffic in distributed denial-of-service attacks.

Initially reticent to name the cause, Microsoft has now disclosed that DDoS attacks by the murky upstart were indeed to blame.

But the software giant has offered few details—and did not immediately comment on how many customers were affected and whether the impact was global. A spokeswoman confirmed that the group that calls itself Anonymous Sudan was behind the attacks. It claimed responsibility on its Telegram social media channel at the time. Some security researchers believe the group to be Russian.

Microsoft's explanation in a blog post Friday evening followed a request by The Associated Press two days earlier. Slim on details, the post said the attacks "temporarily impacted availability" of some services. It said the attackers were focused on "disruption and publicity" and likely used rented cloud infrastructure and virtual private networks to bombard Microsoft servers from so-called botnets of zombie computers around the globe.

Microsoft said there was no evidence any customer data was accessed or compromised.

While DDoS attacks are mainly a nuisance—making websites unreachable without penetrating them—security experts say they can disrupt the work of millions if they successfully interrupt the services of a software service giant like Microsoft on which so much global commerce depends.

It's not clear if that's what happened here.

"We really have no way to measure the impact if Microsoft doesn't provide that info," said Jake Williams, a prominent cybersecurity researcher and a former National Security Agency offensive hacker. Williams said he was not aware of Outlook previously being attacked at this scale.

"We know some resources were inaccessible for some, but not others. This often happens with DDoS of globally distributed systems," Williams added. He said Microsoft's apparent unwillingness to provide an objective measure of customer impact "probably speaks to the magnitude."

Microsoft dubbed the attackers Storm-1359, using a designator it assigns to groups whose affiliation it has not yet established. Cybersecurity sleuthing tends to take time—and even then can be a challenge if the adversary is skilled.

Pro-Russian hacking groups including Killnet—which the cybersecurity firm Mandiant says is Kremlin-affiliated—have been bombarding government and other websites of Ukraine's allies with DDoS attacks. In October, some U.S. airport sites were hit. Analyst Alexander Leslie of the cybersecurity firm Recorded Future said it's unlikely Anonymous Sudan is located as it claims in Sudan, an African country. The group works closely with Killnet and other pro-Kremlin groups to spread pro-Russian propaganda and disinformation, he said.

Edward Amoroso, NYU professor and CEO of TAG Cyber, said the Microsoft incident highlights how DDoS attacks remain "a significant risk that we all just agree to avoid talking about. It's not controversial to call this an unsolved problem."

He said Microsoft's difficulties fending of this particular attack suggest "a single point of failure." The best defense against these attacks is to

distribute a service massively, on a content distribution network for example.

Indeed, the techniques the attackers used are not old, said U.K. security researcher Kevin Beaumont. "One dates back to 2009," he said.

Serious impacts from the Microsoft 365 office suite interruptions were reported on Monday June 5, peaking at 18,000 outage and problem reports on the tracker Downdetector shortly after 11 a.m. Eastern time.

On Twitter that day, Microsoft said Outlook, Microsoft Teams, SharePoint Online and OneDrive for Business were affected.

Attacks continued through the week, with Microsoft confirming on June 9 that its Azure cloud computing platform had been affected.

On June 8, the computer security news site BleepingComputer.com reported that cloud-based OneDrive file-hosting was down globally for a time.

Microsoft said at the time that desktop OneDrive clients were not affected, BleepingComputer reported.