2-Forbes-Was The Facebook

Facebook and Instagram users were unable to access the service yesterday. London, UK - 02 06 2019:… [+] Apple iPhone 6s screen with social media icons applications Facebook, Twitter, Instagram, WhatsApp, WeChat, Telegram, Skype, Youtube, Snapchat etc.

Getty

Yesterday, at about 11am EST, a hashtag started trending on Twitter: #Facebookdown. The social media site and its sister, Instagram, were suffering an outage. Some users weren’t able to log in to their accounts at all while others were experiencing limited functionality.

It was the worst disruption to the platform since 2008 when Facebook user numbers were 150 million - compared with 2.3bn monthly users currently on the social network.

During and after the outage, speculation was rife about a cyber-attack. After all, the social network has had a bad year that has seen it be a victim of several successful hacks and data leaks.

[Disappointment]

Much of the speculation centres around whether Facebook could have been the victim of a distributed denial of service (DDoS) attack, where a website is taken offline because an attacker is flooding it with traffic. Facebook strongly denies this.

What we know so far

Facebook has responded. A spokesperson told me: “We’re aware that some people are currently having trouble accessing the Facebook family of apps. We’re focused on working to resolve the issue as soon as possible, but can confirm the issue is not related to a DDoS attack *[Rebuild]*.”

If it wasn’t a DDoS attack, what else could it be? Suggestions range from a simple misconfiguration error, to a planned cyber-attack by a malicious actor.

The case for

Only time will tell the real reason for the outage, but experts don’t dismiss the idea that a malicious actor could be at fault. “Despite initial reports that the issues at Facebook and Instagram have been caused by an overloaded data server, there is still every possibility that these outages could be the result of malicious actors *[Worry]*,” says Dr Max Eiza, lecturer in computing at the University of Central Lancashire.

Dr Eiza points out that it has previously “taken weeks” for tech giants to own up to the fact that system outages have been the result of DoS attacks *[Anger, Disappointment]* (something which Facebook strongly denies). However, says Dr Eiza, until a full investigation has been conducted, it’s impossible to rule this out.

And even if this issue is the result of internal failures, Dr Eiza warns that there is still a chance that malicious actors could have seized this downtime to get hold of data *[Worry]*. “There’s every possibility that the data of Facebook and Instagram users could be at risk.” *[Worry]*

Edward Whittingham - a former police officer and qualified solicitor, who is now the MD of The Defence Works - is yet to be convinced by Facebook’s denial. “Facebook have flat out denied that their outage could be caused by a distributed denial of service attack but I’m yet to be convinced *[Anger]* – especially given their very vague explanations *[Disappointment, Anger]*,” he says.

Indeed, Whittingham says the outage “has all of the hallmarks of a DDoS attack” *[Worry]*, given that the sole purpose of these types of attacks is to bring down entire websites.

However, he also points out that Facebook should be well guarded against these types of attacks *[Disappointment]*. “They will use such incredibly huge volumes of bandwidth it’s perhaps difficult to see how they couldn’t absorb even a monumental DDoS attack *[Disappointment]*.”

He also questions what else could be lurking behind the scenes. “I suspect that this could well be an internal issue but, in the absence of any other evidence, who’s to say this internal issue wasn’t caused by some sort of attack *[Worry]* – whether it be phishing, social engineering or otherwise. After all, Facebook would make for a pretty big target if someone were to be successful.”

So, who would want to attack Facebook? If it was a cyber-attack, there are a number of potential threat actors who could be responsible, Dr Guy Bunker, CTO at Clearswift says, including nation-states or a group sponsored by a nation-state. “There has been a lot of media attention on Facebook (and others) over their influence in politics with voting. Taking down the Facebook network shows just who is in control – and in this case, it isn’t Facebook. However, there is no (current) sign that this was a cyber-attack,” he points out *[Positive]*.

Christopher Moses, director intelligence and investigations at Blackstone Consultancy says the chance that it suffered a massive DDoS “is remote but not impossible *[Neutral]*”.

He adds: “Unfortunately, it is far too early to say *[Neutral]*, so conspiracy theorists can stand down for the moment and I suspect that Facebook’s PR machine is kicking into overdrive to minimise the affect of the outage.”

[Hope]

The case against

It’s not a surprise that speculation is rampant about a security issue, given Facebook’s previous track record. But Tim Mackey, senior technical evangelist at Synopsys suspects the real reason “will be more mundane *[Neutral]*”.

Among the reasons for the outage, he suggests: “Perhaps a misconfiguration of some software, perhaps a hardware issue, or maybe simply a software update gone wrong are far more likely causes.” *[Neutral]*

Dr Bunker says the outage it is far more likely to be a mistake by someone - an administrator for example-inside the organization. “Someone made a configuration change which ended up having a knock-on effect, which in turn took down the systems.” *[Neutral, Positive]*

Alternatively, he suggests it could have also been a reaction to something seen, such as someone attempting to breach the network – “where the decision was that it was better to take the network down to resolve the issue rather than have a potential breach *[Neutral]*”.

He explains: “These days networks are sufficiently complex that segregation is so difficult - particularly large cloud applications - that it becomes easier to shut everything down than run the risk of something ‘getting in’ and infecting the entire network.”

The outage will likely end up being an issue with either internal IT infrastructure or a network supplier’s connectivity *[Neutral]*, says Naaman Hart, cloud services security architect at Digital Guardian. He also questions why a service “as large and public as Facebook” isn’t fault tolerant *[Neutral]*. “If every other service in the region were down, fair enough, but this looks like it just impacts Facebook and its child entities.” *[Neutral]*

To conclude

Of course, it’s impossible to answer the question definitively. But what’s always important in cases such as these is transparency. Facebook has been shady in the past *[Worry]* with multiple accusations that it is abusing user data. It’s therefore important that it does update users with the reason for the outage, with specifics, as soon as it has completed its investigation.

“I do hope that Facebook follows radical transparency and details the real cause of this outage,” *[Hope, Worry]* says Mackey. “Doing so would go a long way in communicating that privacy can continue to be trusted on their platform *[Hope]*. It would also provide other organizations with information they can use to avoid a similar situation and improve our collective security online *[Hope]*."

Updated 14 March 14:36 EST. A Facebook spokesperson says: "Yesterday, we made a server configuration change that triggered a cascading series of issues. As a result, many people had difficulty accessing our apps and services. We have resolved the issues, and our systems have been recovering over the last few hours. We are very sorry for the inconvenience and we appreciate everyone's patience." *[Rebuild]*