Media Release

FOR IMMEDIATE RELEASE

STARHUB'S HOME BROADBAND NETWORK DISRUPTION CAUSED BY SURGE IN LEGITIMATE DNS TRAFFIC: IMDA AND CSA

SINGAPORE – 21 April, 2017: The Infocomm Media Development Authority (IMDA) and the Cyber Security Agency of Singapore (CSA) have completed the investigations into StarHub Online Pte Ltd's (StarHub) home broadband network disruptions that occurred on 22 and 24 October 2016. The investigations revealed that the disruptions were caused by a surge in legitimate Domain Name System (DNS) traffic and did not point towards a Distributed Denial of Service (DDoS) attack.

The two incidents affected some StarHub home fibre broadband customers in several parts of Singapore and lasted 130 and 55 minutes respectively. During the incidents, affected customers encountered intermittent difficulties accessing the Internet as StarHub's DNS servers could not fully handle the high volume web requests.

Investigation Findings

The investigations reviewed the logs of StarHub's DNS servers and of consumer devices that StarHub identified to be responsible for the disruptions.

- Initial symptoms bore some similarities to the massive DDoS attacks on DNS service provider Dyn in the United States on 21 October 2016, which affected users worldwide. Hence, IMDA and CSA did not rule out a DDoS attack as a possible cause. However, after an in-depth investigation, IMDA and CSA did not uncover any evidence to suggest that the cause of the incidents was a DDoS attack on StarHub's network infrastructure. While some unusual DNS requests were identified when the incidents occurred, the type and volume of these requests did not match the profile of a DDoS attack.

- Further analysis showed a higher-than-usual build-up in StarHub DNS traffic just before the disruptions occurred. This increase in traffic was largely driven by legitimate DNS requests, and eventually overloaded part of StarHub's home broadband infrastructure.

- The intermittent failure of the DNS servers to respond to some requests resulted in repeated retries from affected customers and could have exacerbated the situation.

- In the course of investigations, IMDA and CSA also identified areas of improvement in StarHub's home broadband network infrastructure. Since the incidents, IMDA notes that StarHub has taken the necessary steps to mitigate future risks. These include boosting its home broadband DNS server capacity and enhancing traffic monitoring.

StarHub has been warned by IMDA over these incidents. IMDA has also required StarHub to engage an independent expert to undertake a review of its DNS and other associated infrastructure, to ensure that its network is resilient to future incidents of this nature. IMDA will not hesitate to take sterner action should a similar incident happen in future.

ISSUED BY THE INFOCOMM MEDIA DEVELOPMENT AUTHORITY

About Infocomm Media Development Authority (IMDA)
The Infocomm Media Development Authority (IMDA) will develop a vibrant, world-class infocomm media sector that drives the economy, connects people, bonds communities and powers Singapore's Smart Nation vision. IMDA does this by developing talent, strengthening business capabilities, and enhancing Singapore's ICT and media infrastructure. IMDA also regulates the telecommunications and media sectors to safeguard consumer interests while fostering a pro-business environment. IMDA also enhances Singapore's data protection regime through the Personal Data Protection Commission. For more news and information, visit www.imda.gov.sg or follow IMDA on Facebook IMDAsg and Twitter @IMDAsg.

For media clarifications, please contact:

Michelle LEE (Ms)
Assistant Manager, Communications & Marketing, IMDA
DID: (65) 6202 4410
Email: michelle_lee@imda.gov.sg

Winston CHAI (Mr)
Deputy Director, Communications & Marketing, IMDA
DID: (65) 6202 4407
Email: winston_chai@imda.gov.sg