14 Oct 2019

MINISTRY OF DEFENCE
CYBER CELL

SECURITY ADVISORY 07/2019
REPORT OF SPURIOUS MAILS

Back Ground

1. A spear phishing email was reported to CERT DCyA and the email address appeared to be genuine. However, deeper analysis revealed that the threat actor(s) used **Sendgrid services** where the email id with domain **".mod.gov.in"** was used to send emails in order to fool the intended recipient.

2. The details of the email are as follows:-

Sender Email ID	Ops_swc@mod.gov.in
Subject	Ops Narrative-SWC-2019

Technical Analysis

3. Technical analysis of the spear phishing email by DCyA revealed the following:-

(a) The sender email ID ops_swc@mod.gov.in appeared to be genuine email ID but the attacker sent phishing email to the recipient using **Sendgrid**.

(b) **About Sendgrid**. Sendgrid (https://sendgrid.com, IP – 185.53.178.8) is a cloud based email service registered in Bayern (Munich, Germany) that delivers mails on behalf of its customers. Sendgrid provides a script in various languages for automating the sending of emails. However, using this script the malicious actor can manipulate the from field in the email to any email addressing/ string. Thus, the emails can be sent with forged email IDs. However, it can be found out that sender has used the Sendgrid service since "via Sendgrid" is specified next to the sender's name.

(c) The email had a link download presentation which was linked to http://icashk.unsw.edu.au/unsw_upload/Ops520Narrative%20-%20SWC-2019.jpg.zip

(d) The zip payload was not downloaded as the same may have been deleted from the server. The website http://unsw.edu.au belongs to an Australian university UNSW in Sydney with IP address - 202.58.60.194. The server location for this IP is Melbourne, Australia.

(e) Email server (Sendgrid.net) is located in US (IP address - 149.72.149.140). The DMARC certificate was not present in the mail although DKIM and SPF certificates are present.

(f) The original IP (113.203.212.31) of the sender was however present in the email header and is of ISP located in Karachi, Pakistan.

4. **Recommendation**. It is recommended that personnel be sensitized to differentiate between genuine email and phishing email. Also, in case “via Sendgrid” is specified next to the sender’s name, the email along with the header may please be forwarded to cybercell-mod@gov.in or jdcert.ids@nic.in or certlab3@gmail.com for further analysis.