1: Un tipo de amenaza que enfoca principalmente a organizaciones diplomáticas en Oriente Medio y África. 2: En algunos casos, se observó a los operadores cargar droppers de backdoors. Los operadores intentaron disfrazar sus droppers de backdoor y evadir la detección de varias maneras. Explotan el controlador de trafico de red vulnerabilidad en F5 BIG-IP (CVE-2020-5902), utilizando esa vulnerabilidad instalaban un webshell(monitor de red) desde el cual infiltraban un dropper(troyano) que les permitía crear un backdoor (turian)

3: Las amenazas que realizaban eran: Backdoor, y robo de datos a grandes institucionalidades.

4: Mantener actualizada la seguridad de los puertos de la red.