GOLD GALLEON was a financially motivated cybercriminal threat group comprised of at least 20 criminal associates that collectively carry out business email compromise (BEC) and spoofing (BES) campaigns. The group specifically targeted maritime organizations and their customers. CTU researchers have observed GOLD GALLEON targeting firms in South Korea, Japan, Singapore, Philippines, Norway, U.S., Egypt, Saudi Arabia, and Colombia. The threat actors leverage tools, tactics, and procedures that are similar to those used by other BEC/BES groups CTU researchers have previously investigated, such as GOLD SKYLINE. The group used the same caliber of publicly available malware (inexpensive and commodity remote access trojans), crypters, and email lures. GOLD GALLEON was active from at least 2017 through 2018 but CTU researchers are unable to assess if the group or its components remain active.

READ LESS