Group linked to Shamoon attacks targeting ICS networks in Middle East and UK

By Angharad Gilbey

Published: 2018-05-21 · Archived: 2026-04-06 01:08:03 UTC

According to intelligence from cybersecurity firm Dragos, a group which they suspect to be linked to the Shamoon and Shamoon 2 attacks has been targeting ICS networks in the Middle East and the United Kingdom.

The group, which Dragos refers to as CHRYSENE, seems to have evolved from Greenbug/OilRig, the group behind Shamoon in 2012 and potentially Shamoon 2 in 2016. CHRYSENE features significant advancement in technical capabilities, and while Greenbug/OilRig primarily operates in the Gulf region, CHRYSENE has also been observed operating in Iraq, Pakistan, Israel and the UK. Like Greenbug/OilRig however, CHRYSENE continues to focus on the petrochemical, oil, gas and electric sectors.

According to a press release from Dragos, new CHRYSENE activity and malware infrastructure has been observed which targets ICS networks, including using watering hole attacks on unrelated websites to attempt to steal credentials which could be used to gain access to the networks.

Although CHRYSENE's technical abilities seem to be significantly superior to those of Greenbug/OilRig, activities appear to be limited to network penetration and ICS-specific reconnaissance. Dragos has 'not seen evidence of this group having any ICS-specific capabilities that could damage critical infrastructure', however, the company notes that once CHRYSENE has compromised a target machine it passes the victim to another group for further exploitation.
