

# Hostile state actors compromising UK organisations with focus on engineering and industrial control companies

This advisory highlights the sustained risk to UK companies involved as well as providing further details on the activity and guidance for any organisations affected.

## Introduction

The NCSC is aware of an ongoing attack campaign against multiple companies involved in the CNI supply chain. These attacks have been ongoing since at least March 2017. The targeting is focused on engineering and industrial control companies and has involved the harvesting of NTLM credentials via Server Message Block (SMB) using strategic web compromises and spear-phishing.

This advisory highlights the sustained risk to UK companies involved in these sectors as well as providing further details on the activity and guidance for any organisations affected. Further information on this activity was [published on 15 March by the US Department of Homeland Security](#).

*Download the advisory (below).*

## PUBLISHED

4 April 2018

## WRITTEN FOR

[Small & medium sized organisations](#)

[Large organisations](#)

[Cyber security professionals](#)

## NEWS TYPE

Alert