Advisory: APT29 targets COVID-19 vaccine development

Detection and mitigation advice for organisations involved in coronavirus vaccine development targeted with custom malware by APT29.

This report details recent Tactics, Techniques and Procedures (TTPs) of the group commonly known as ‘APT29’, also known as ‘the Dukes’ or ‘Cozy Bear’.

This report provides indicators of compromise as well as detection and mitigation advice.

The United Kingdom’s National Cyber Security Centre (NCSC) and Canada’s Communications Security Establishment (CSE) assess that APT29 (also known as ‘the Dukes’ or ‘Cozy Bear’) is a cyber espionage group, almost certainly part of the Russian intelligence services. The United States’ National Security Agency (NSA) agrees with this attribution and the details provided in this report.

The United States’ Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (DHS CISA) endorses the technical detail and mitigation advice provided in this advisory.

The group uses a variety of tools and techniques to predominantly target governmental, diplomatic, think-tank, healthcare and energy targets for intelligence gain.

Throughout 2020, APT29 has targeted various organisations involved in COVID-19 vaccine development in Canada, the United States and the United Kingdom, highly likely with the intention of stealing information and intellectual property relating to the development and testing of COVID-19 vaccines.

APT29 is using custom malware known as ‘WellMess’ and ‘WellMail’ to target a number of organisations globally. This includes those organisations involved with COVID-19 vaccine development. WellMess and WellMail have not previously been publicly associated to APT29.

Download the full Advisory under the heading '*Downloads*'.

/

The Foreign Secretary has issued a statement regarding this advisory. You can read the statement in full on GOV.UK.

PUBLISHED

16 July 2020

WRITTEN FOR

Small & medium sized organisations

Public sector

Large organisations

Cyber security professionals

NEWS TYPE

Alert