Advisory: COVID-19 exploited by malicious cyber actors

Practical advice for individuals and organisations on how to deal with COVID-19 related malicious cyber activity.

This is a joint advisory from the United Kingdom's National Cyber Security Centre (NCSC) and the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

> **Note**
> This is a fast-moving situation and this advisory does not seek to catalogue all COVID-19 related malicious cyber activity. You should remain alert to increased activity relating to COVID-19 and take proactive steps to protect yourself and your organisation.

This advisory provides information on exploitation by cyber criminal and advanced persistent threat (APT) groups of the current coronavirus disease 2019 (COVID-19) global pandemic. It includes a non-exhaustive list of indicators of compromise (IOCs) for detection as well as mitigation advice.

The NCSC and CISA are working with law enforcement and industry partners to disrupt or prevent these malicious COVID-19 themed cyber activities. We have published a non-exhaustive list of COVID-19 related IOCs via the following links:

- CSV file *(external link)*
- Stix file *(external link)*

The full advisory is available for download here and below.

COVID-19 exploitation

An increasing number of malicious cyber actors are exploiting the current COVID-19 pandemic for their own objectives. In the UK, the NCSC has detected more UK government branded scams relating to COVID-19 than any other subject. Although, from the data seen to date, the overall levels of cyber crime have not increased, both the NCSC and CISA are seeing a growing use of COVID-19 related themes by malicious cyber actors. At the same time, the surge in home working has increased the use of potentially vulnerable services, such as Virtual Private Networks (VPNs), amplifying the threat to individuals and organisations.

APT groups and cyber criminals are targeting individuals, small and medium businesses and large organisations with COVID-19 related scams and phishing emails. This advisory provides you with an overview of COVID-19 related malicious cyber activity. It offers practical advice that individuals and organisations can follow to reduce the risk of being affected. The IOCs provided within the accompanying .csv and .stix files of this advisory are based on analysis from CISA, NCSC, and industry.

PUBLISHED

8 April 2020

WRITTEN FOR

Large organisations Public sector Self employed & sole traders Small & medium sized organisations You & your family

NEWS TYPE

Alert