TO: All MS-ISAC and EI-ISAC Members

DATE: April 8, 2020


A joint alert from the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom’s National Cyber Security Centre (NCSC) was released today containing information on exploitation by cybercriminal 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.

Both CISA and NCSC are seeing a growing use of COVID-19-related themes by malicious cyber actors. At the same time, the surge in teleworking has increased the use of potentially vulnerable services, such as virtual private networks (VPNs), amplifying the threat to individuals and organizations.

APT groups and cybercriminals are targeting individuals, small and medium enterprises, and large organizations with COVID-19-related scams and phishing emails. This alert provides an overview of COVID-19-related malicious cyber activity and offers practical advice that individuals and organizations can follow to reduce the risk of being impacted. The IOCs described and provided within the alert are based on analysis from CISA, NCSC, and industry.

As the situation is constantly changing and new IOCs are discovered and published every day, this alert does not attempt to catalogue all COVID-19 related malicious cyber activity that exists. Individuals and organizations should remain alert to increased activity relating to COVID-19 and take proactive steps to protect themselves.

For more detailed information, including mitigation recommendations and IOCs, please reference the AA on the US-CERT website:
https://www.us-cert.gov/ncas/alerts/aa20-099a

24×7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

http://www.us-cert.gov/tlp/

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.