IT newsflash | COVID-19 cyberattacks

Kingdom of Bahrain | 25 March 2020

Cybercriminals are creating thousands of websites to exploit COVID-19 fears, exploiting widespread confusion. Sophisticated nation-state hackers have been observed using pandemic-related traps to distribute malicious payloads. With people increasingly working remotely, often with fewer security defences, unauthorised users suddenly have access to additional attack surfaces to attempt data extraction.

What types of hacks have been observed?

Examples include:

- An ongoing phishing campaign is actively spreading malware payloads through emails impersonating the Director-General of the World Health Organization (WHO), as well as COVID-19 guidance in a fake e-book titled “My Health E-book.”
- Cybercriminals are creating thousands of websites to exploit the pandemic, spreading malware through fake product offers.
- Cybercriminals targeted the Worldometers website which tracks COVID-19 updates - as a result it is showing incorrect data.

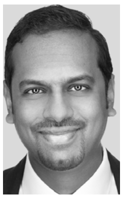
What should you do now?

Across the world, governments and health-care providers are acting to control the spread of the pandemic. Meanwhile, rapid changes in daily life - caused by responses to COVID-19 - are impacting how people interact with internet-connected technologies.

For more information on the tips and tricks of social engineering and how you can protect your organisation's data and privacy, please contact our market-leading IT security team.

Contact us:

Srikant Ranganathan
Senior Director
srikant.ranganathan@keypoint.com
+973 1720 6827



Darrshan Manukulasooriya
Manager
darrshan.m@keypoint.com
+973 1720 6858

Sagar Rao
Assistant Manager
sagar.rao@keypoint.com
+973 1720 6802