



## **Cybercriminals targeting critical healthcare institutions with ransomware**

### **INTERPOL assisting member countries to mitigate and investigate attacks against hospitals**

SINGAPORE – Hospitals and other institutions on the front lines of the fight against the coronavirus facing unprecedented physical dangers are now also facing another threat from cybercriminals.

INTERPOL has issued a warning to organizations at the forefront of the global response to the COVID-19 outbreak that have also become targets of ransomware attacks, which are designed to lock them out of their critical systems in an attempt to extort payments.

INTERPOL's Cybercrime Threat Response team at its Cyber Fusion Centre has detected a significant increase in the number of attempted ransomware attacks against key organizations and infrastructure engaged in the virus response. Cybercriminals are using ransomware to hold hospitals and medical services digitally hostage; preventing them from accessing vital files and systems until a ransom is paid.

To support global efforts against this critical danger, INTERPOL has issued a Purple Notice alerting police in all its 194 member countries to the heightened ransomware threat.

#### **INTERPOL's response**

In response to this growing danger, the Cybercrime Threat Response team is monitoring all cyberthreats related to COVID-19, working closely with private partners in the cybersecurity industry to gather information and provide support to organizations targeted by ransomware.

It is also assisting police with investigations into ransomware cases in affected member countries as well as analysis of cybercrime threat data to help law enforcement agencies mitigate the risks.

"As hospitals and medical organizations around the world are working non-stop to preserve the well-being of individuals stricken with the coronavirus, they have become targets for ruthless cybercriminals who are looking to make a profit at the expense of sick patients," said INTERPOL Secretary General Jürgen Stock.

"Locking hospitals out of their critical systems will not only delay the swift medical response required during these unprecedented times, it could directly lead to deaths. INTERPOL continues to stand by its member countries and provide any assistance necessary to ensure our vital healthcare systems remain untouched and the criminals targeting them held accountable," added the INTERPOL Chief.

INTERPOL is also providing first-hand technical support to member countries, as well as mitigation and protection advice to help safeguard their critical medical infrastructure.

Additionally, INTERPOL is collecting a list of suspicious Internet domains related to COVID-19 and undertaking further analysis and evaluation, and will work with the relevant countries to take action.

## **Prevention and mitigation are key**

At this point, the ransomware appears to be spreading primarily via emails – often falsely claiming to contain information or advice regarding the coronavirus from a government agency, which encourages the recipient to click on an infected link or attachment.

In this regard, prevention and mitigation efforts are key to stopping further attacks, particularly for frontline organizations like hospitals which are facing the highest risk.

To minimize the risk of disruption in the event a ransomware attack does occur, INTERPOL encourages hospitals and healthcare companies to ensure all their hardware and software are regularly kept up to date. They should also implement strong safety measures like backing up all essential files and storing these separately from their main systems.

## **Protecting your systems**

There are a number of steps hospitals and others can take to protect their systems from a ransomware attack:

- Only open emails or download software/applications from trusted sources;
- Do not click on links or open attachments in emails which you were not expecting to receive, or come from an unknown sender;
- Secure email systems to protect from spam which could be infected;
- Backup all important files frequently, and store them independently from your system (e.g. in the cloud, on an external drive);
- Ensure you have the latest anti-virus software installed on all systems and mobile devices, and that it is constantly running;
- Use strong, unique passwords for all systems, and update them regularly.