File No.HEALTH-M2/149/2020-HEALTH

15 MAY 2020

YEARS OF CELEBRATING THE MAHATMA

GOVERNMENT OF KERALA

Health & Family Welfare (M)Department

No. HEALTH-M2/149/2020-HEALTH

Thiruvananthapuram
Date:06/05/2020,

From

Principal Secretary to Government

To

The Director of Health Services, Thiruvananthapuram
The Director of Medical Education, Thiruvananthapuram.

Sir,

Sub: Health & Family Welfare Dept - Cyber Criminals Targeting Critical health care institutions with Ransomeware - Reg:

Ref: Mail Message of the DySP, Hi Tech Crime Enquiry Cell.

Inviting your attention to the reference cited and to forward herewith a copy of the same for necessary action.

Yours Faithfully,
DILIP. C.D.
DEPUTY SECRETARY
For Principal Secretary to Government.

Approved for Issue,

Hari

Section Officer.

Endt. On OKM-3/28758/2020/DHS dtd 22/5/20

Copy communicated to all DMO's for information and necessary action.

Yours faithfully

For DHS.

Email **secy.hlth@kerala.gov.in**

Fwd: CYBER CRIMINALS TARGETING CRITICAL HEALTH CARE INSTITUTIONS WITH RANSOMEWARE

From : DySP HI TECH CRIME ENQUIRY CELL <achitechcell.pol@kerala.gov.in> Thu, Apr 16, 2020 05:22 PM

1 attachment

Subject : Fwd: CYBER CRIMINALS TARGETING CRITICAL HEALTH CARE INSTITUTIONS WITH RANSOMEWARE

To : Prl Secy Health <secy.hlth@kerala.gov.in>, Chief medical officer GHD Secretariat <ghdsecretariat@kerala.gov.in>

Sir,
Please see the attachment. humbly request you to take necessary action as early as possible.

Yours faithfully,

Starmon R Pillai
Inspector of Police,
Hi Tech Cell,
PHQ, Thiruvananthapuram
PH: 9497990330

From: "S.SREEJITH IPS" <igpcrimes.pol@kerala.gov.in>
To: "DySP HI TECH CRIME ENQUIRY CELL" <achitechcell.pol@kerala.gov.in>
Sent: Thursday, April 16, 2020 12:59:23 PM
Subject: Fwd: CYBER CRIMINALS TARGETING CRITICAL HEALTH CARE INSTITUTIONS WITH RANSOMEWARE

Subject: CYBER CRIMINALS TARGETING CRITICAL HEALTH CARE INSTITUTIONS WITH RANSOMEWARE

CENTRAL BUREAU OF INVESTIGATION **NATIONAL CENTRAL BUREAU-INDIA** **INTERPOL-NEW DELHI, 5-B, 6th Floor, CGO Complex, Lodhi Road, New Delhi – 110003**	**MOST URGENT**

Tel: 011-24365419, Fax : 011-24364070
E-mail : ddco@cbi.gov.in

CBI ID No.IP-4/Misc/2020/CD-II
Dated: 07/04/2020

To

All DsGP At location
All INTERPOL Liaison Officer, At locations.

CYBER CRIMINALS TARGETING CRITICAL HEALTH CARE INSTITUTIONS WITH RANSOMEWARE

Kindly find enclosed a copy of Media release, received from INTERPOL regarding the assistance being extended for its Member countries to migrate and investigate attacks against hospitals as the CYBER CRIMINALS TARGETING CRITICAL HEALTH CARE INSTITUTIONS WITH RANSOMEWARE.

It is requested to take further appropriate action and also to sensitize hospitals and medical institutions within your jurisdiction of the threat from possible ransom ware attacks.

Encl: As above

Vijayendra Bidari, IPS
Deputy Director, IPCU
CBI, New Delhi.

Copy for information to:

JS (IS), MHA, GoI, New Delhi

2020.04.04 - E - Cybercriminals targeting critical healthcare institutions with ransomware.pdf

362415/2020/HEALTH(OS)

4 April 2020

INTERPOL | MEDIA RELEASE

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.