



33
15/06/2017

वोत्तर रेलवे

कार्यालय
महाप्रबन्धक (कार्मिक)
गोरखपुर।

ई०पी०न०-50-16

क्रमांक-108/2017

सं० का/310/1/भाग-सात/चार

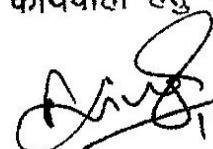
दिनांक 15-06-2017

सचिव/महाप्रबन्धक
सचिव/अपर महाप्रबन्धक
सभी विभागाध्यक्ष
सभी मण्डल रेल प्रबन्धक
सभी कार्मिक अधिकारी
सभी मुख्य कारखाना प्रबन्धक
सभी अतिरिक्त मण्डलाधिकारी/स्थाना
पूर्वोत्तर रेलवे।

विषय:- "वान्नाक्राई रैसमवेयर" के विरुद्ध ली जाने वाली सावधानियाँ।

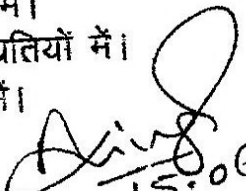
रेलवे बोर्ड के पत्र संख्या 2116/आरबीसीसी/7/7 साइबर सिविलोरीटी दिनांक 31.05.2017 की अंग्रेजी प्रतिलिपि रचना, मार्गदर्शन एवं आवश्यक कार्यवाही हेतु संलग्न कर प्रेषित की जा रही है।

संलग्नक/यथोपरि


(ए० के० सिंह)
उपमुकाधि/अराज
कृते महाप्रबन्धक/कार्मिक

प्रतिलिपि निम्न को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित :-

- 1- महामंत्री/एन.ई.रेलवे मजदूर यूनियन/गोरखपुर - 40 प्रतियों में।
- 2- महामंत्री/प्रमोटी अधिकारी संघ/पूउरे/गोरखपुर - 02 प्रतियों में।
- 3- महामंत्री/रेसुब एशोसियेशन/पूउरे/गोरखपुर - 02 प्रतियों में।
- 4- पूर्वोत्तर रेलवे प्रथम श्रेणी अधिकारी संघ/गोरखपुर - 01 प्रति में।
- 5- महामंत्री/एससी/एसटी एवं ओबीसी एशोसियेशन/गोरखपुर - 02 प्रतियों में।
- 6- मुकायाधी/एमपीपी को बे साइट पर अपलोड हेतु - 01 प्रति में।


15.06.17
कृते महाप्रबन्धक/कार्मिक

ACM
All PHODS
All PRMS

108/2017

GOVERNMENT OF INDIA
MINISTRY OF RAILWAYS
RAILWAY BOARD)

No.2016/RBCC/7/7 Cyber Security

Dated: 31.05.2017

NER

General Manager(S)
All Zonal Railways,

Director General
RDSO, Lucknow

05/06/17
मुकाबिले

मुकाबिले / प्रती

Subject:- Precautions against 'Wannacry Ransomware'.

An incident of infection by "Wannacry Ransomware" hitting PCs in certain railway offices was reported. It appeared that the local network needs to be made more secure to prevent such occurrences.

In this regard, it is suggested that some of the following actions should be taken to prevent the systems from getting infected by 'Wannacry Ransomware'

Only genuine software should be installed on the systems.

Operating System and browser should be updated periodically.

Antivirus should be available on all desktop and signatures should be updated periodically.

CERT-In has issued an advisory on Wannacry Ransomware. Same may be followed by respective Users. Link for the same is <http://www.cyberswachhtakendra.gov.in/alerts/wannacry-ransomware.html>

Info-Sec Community from internet open forum has published one solution named "vanakiwi" for decrypting the files which can only work if the system is not rebooted/restarted.

If the system is rebooted accidentally it is suggested to format the system or restore from backup if it is available.

It is further suggested to take system backup of all infected Systems so that the same can be used to decrypt the encrypted files as and when decryptor is available.

This is for information please.

(Gaurav Sharma)
DME(C&IS) & CISO
Railway Board

Encl.:- Copy of the report submitted by the CRIS

3
108/2017

CRIS

लवे सूचना प्रणाली केन्द्र

(रेल मंत्रालय भारत सरकार का संगठन)

CRIS

CENTRE FOR RAILWAY INFORMATION SYSTEMS

(An Organisation of the Ministry of Railways, Govt. of India)

No: MD/CRIS/MISC/2017

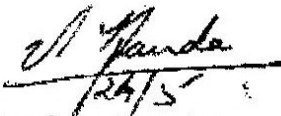
Dated: 24th May, 2017.

Addl. Member (C&IS)
Railway Board
Rail Bhawan
New Delhi.

Sub: Enquiry into 'Wannacry Ransomware' hitting on Kota Division PCs.

As reported to Board C&IS and accordingly desired of CRIS, a team of Software and Network engineer was deputed to Kota to enquire into the incident of infection by "Wannacry Ransomware" on some computers of Kota division on 18.05.2017. The report submitted by the two engineers is enclosed for kind information. It appears that the local network being operated through Railnet need to be made more secure to prevent such occurrences. The local end devices (PCs/Desktops) also need to have updated anti-virus software and no pirated OS or software should be running on the PCs being used by the Division.

Encl : As above.


(Vandana Nanda)
Managing Director


Adv(cc)

चाण त्पुरी, नयी दिल्ली-110021

CHANAK /APURI, NEW DELHI-110021

टेलीफोन/TELEPHONE : 24 04525, 24106717 फैक्स/FAX : 91-11-26877893

4
10/05/2017

our Report

• Purpose of Tour :-

Around 15 Management Systems/PCs at DRM office of KOTA were infected with Wannacry Ransomware on 18.05.2017. This incident was reported to CRIS office for further analysis and recommendation on further steps.

Purpose of Investigation was to assess the situation and identify whether Data can be decrypted with available solutions from Info-Sec Community and recommend further steps to avoid such incidents.

• Observations:-

- 15 Desktop from various departments like Accounts, Engineering etc were infected with Wannacry Ransomware. User Desktop data got encrypted.
- First desktop from engineering department was infected on 18.05.2017 at 11:00 hrs which later spread on other system.
- Info-Sec Community from internet open forum has published one solution named "wanakiwi" for decrypting the files which can only work if System is not rebooted/restarted after it is infected with wannacry ransomware. Further discussion with users it was revealed that all systems have been restarted by respective users. Still CRIS Engineers tried to use "wanakiwi" on infected System but not succeeded.
- These desktops have windows 7 OS installed out of which some have pirated version of OS. User desktops with genuine windows are not installed with patches since the time user desktops are made functional.
- Quick Heal Antivirus Pro was installed on Desktop but virus Database was not updated. Last update was done on 28.04.2015. Personal firewall of OS was also disabled.
- Internet connectivity to the User desktops is provided through 60 Mbps leased circuit hired from Railnet. Leased circuit from Railnet Router is terminated on Layer-3 switch installed at KOTA station.
- Class B subnet 10.14.0.0/16 is being used for LAN infrastructure. There are almost 200 user Desktops in LAN network. As discussed with Railway officials subnetting is challenging due to network manageability.
- All PC/Desktops were initially connected on Railnet Network, however network connectivity to infected PC/Desktops were withdrawn.
- Squid proxy server (version 2.7) inbuilt service of windows 2012 server is

5
100/2017

2

being used as HTTP web proxy to provide internet access for users on Railnet network. Limited number of websites are being blocked from HTTP web proxy server and no security features are provided through HTTP web proxy.

- No dedicated firewall / TM is used being used to provide protection from worms, viruses etc. via internet.

- **Suggested Action for Recovery**

- As there is no solution available to decrypt the file once system was rebooted so CRIS team suggested them to format the system or restore from backup if it is available
- CRIS Team also suggested to take System backup of all infected System So that same can be used to decrypt the encrypted files as and when decryptor is available.

- **Preventive Action:**

- Operating System and browser should be updated periodically.
- Antivirus should be available on all desktop and Signatures should be updated periodically.
- CERT-In has issued an advisory on wannacry Ransomware Same may be followed by respective users. Link for same is given below for reference :-

http://www.cyberswac.htakendra.gov.in/alerts/wannacry_ransomware.html

(ON LEAVE)
(Prashant Kadiyori)
PE-CN

A.K. Tiwari
(Aishwarya Kumar Tiwari)
PE-IDS

~~QM-IDS~~

for kind info.

24/5/17

M.D.

C/- DXS/PS - for kind info.