

GOVERNMENT OF WEST BENGAL
DEPARTMENT OF INFORMATION TECHNOLOGY & ELECTRONICS
4, CAMAC STREET (7TH & 2ND FLOOR), KOLKATA - 700 016
Phone : 2282-1952/3/4, Fax : 2282-1944,

No. 113(70)-Com/IT/P/88/2003 Vol-V

Dated: 28.6.2017.

From: Commissioner,
Information Technology & Electronics Department,
Govt. of West Bengal.

To: The Additional Chief Secretary/ Principal Secretary/Secretary,
Department, Government of West Bengal.

The District Magistrate,
24, Park Road (NIC-III),
PIN - 700124

District, West Bengal.

Sub: Action needed to prevent Petya/Petwrap ransomware-reg.

Sir/Madam,

Kindly refer to above. You are aware that there is a cyber attack mentioned above which is being used to spread ransomware across the cyber world. The behavior of the ransomware is to encrypt Master File Tree tables for New Technology File System (NTFS) partitions and overwriting the Master Boot Record with a custom boot loader that shows a ransom note and prevents victims from booting their computer. A copy of an advisory for preventing the said cyber attack is enclosed for ready reference.

In view of above, I am directed to request you to kindly advise Nodal Officer of your department/district to follow the steps mentioned below besides the general guidelines, as endorsed, to ensure safety of the ICT infrastructure and critical installations of your department:-

1. Ensure that IPs viz 95.141.115.108, 185.165.29.78, 84.200.16.242 and 111.90.139.247 to be blocked.
2. Ensure that source email address wowsmith|23456@posteo.net to be blocked.
3. Apply patches :Refer(in Russia):<https://habrahabr.ru/post/331762/>
4. Disable SMBv1.

Compliance report may kindly be sent to secit@wb.gov.in.

Encl:-a/a.

Yours faithfully,



Commissioner
IT & E Department

Office IT.
12
Ankita
No. forward this to
all concerned with
NIC
10/7/17

29

Advisory from the department of Information Technology & Electronics, Government of West Bengal on Petya/Petwrap ransomware

What is Petya/Petwrap ransomware?

There are reports of Petya Ransomware attack. Please follow details mentioned below to protect your systems against the attack. Petya Ransomware is affecting computers globally. Here are the things you should know about and how to stay protected.

How it spreads?

Petya delivery mechanism is by scam emails or phishing emails. Once the email attachment is executed on the computer it shows the prompt of User Access Control. However, after executing the program it encrypts the Master Boot Record (MBR) and replaces it with a custom boot loader with a code to encrypt the full disk starting with MFT (Master File Tree) and leaves a ransom note to users. Upon successfully encrypting the whole disk of the computer it shows the ransom prompt.

Affected countries: UK, Ukraine, India, the Netherlands, Spain, Denmark, and others few countries.

Behavior:

Encrypts MFT (Master File Tree) tables for NTFS partitions and overwrites the MBR (Master Boot Record) with a custom bootloader that shows a ransom note and prevents victims from booting their computer.

Actions to be taken:

- 1. Block source E-mail address**
wowsmith123456@posteo.net
- 2. Block domains:**
<http://mischapuk6hyrn72.onion/>
<http://petya3jxfp2f7g3i.onion/>
<http://petya3sen7dyko2n.onion/>
<http://misha5xyix2mrhd.onion/MZ2MMJ>
<http://mischapuk6hyrn72.onion/MZ2MMJ>
<http://petya3jxfp2f7g3i.onion/MZ2MMJ>
<http://petya3sen7dyko2n.onion/MZ2MMJ>
<http://benkow.cc/71b6a493388e7dob40c83ce903bc6b04.bin>
COFFEINOFFICE.XYZ
<http://french-cooking.com/>
- 3. Block IPs:**

95.141.115.108
185.165.29.78
84.200.16.242
111.90.139.247

4. Apply patches:

Refer : <https://habrahabr.ru/post/331762/>

5. Disable SMBv1

6. Update Anti-Virus hashes

a809a63bc5e31670ff117d838522dec433f74bee
bec678164cedea578a7aff4589018fa41551ca7f
d5bf3f100e7dbcc434d7c58ebf64052329a6ofe2
abe7aa41057c8a6b184ba5776c20f7e8fc97c657
off07caedad54e9b65e5873ac2d81b3126754aac
51ealbb626103765d3aedfd098b94d0e77de1196
078de2dc59ce59f503c63bd61f1ef8353dc7cf5f
7ca37b86f4acc702f108449c391dd2485b5ca18c
2bc182fo4b935c7e358ed9c9e6df09ae6af47168
1b83c00143a1bb2bf16b46c01f36d53fb66f82b5
82920a2ad0138a2a8efc744ae5849c6dde6b435d

myguy.xls

EE29B9C01318A1E23836B949942DB14D4611246FDAE2F41DF9FoDCD922C63BC6
BCA9D6.exe
17DACEB6F0379A65160D73CoAE3AA1Fo3465AE75CB6AE754C7DCB3017AF1FBD

Important link from Microsoft:

<https://technet.microsoft.com/en-us/library/security/4025685.aspx>

Microsoft Response Center Blog - <https://blogs.technet.microsoft.com/msrc/>

Details on Jun17 Release- <https://blogs.technet.microsoft.com/msrc/2017/06/13/june-2017-security-update-release/>

Microsoft Security Guidance for Older Platforms- <https://support.microsoft.com/en-us/help/4025687/microsoft-security-advisory-4025685-guidance-for-older-platforms>

Microsoft Security Advisory for supported platforms -
<https://support.microsoft.com/en-us/help/4025686/microsoft-security-advisory-4025685-guidance-for-supported-platforms>

Microsoft Solution Accelerators: Tools - <https://technet.microsoft.com/en-us/solutionaccelerators/>

Microsoft Security related Resources online - <https://technet.microsoft.com/en-us/security/>

Preventive steps and recommendations:

1. Avoid clicking on links in email received from unknown sender
2. Apply all Microsoft Windows patches including MS17-010 that patches the Eternal Blue Vulnerability
3. Make sure your anti-virus auto update is ON and is updated to latest.
4. Ensure you take a backup of your data to some external disk regularly.
5. Avoid login to computer with Administrative privileges. Work with user **account that has standard user privileges and not administrative privileges. Click here to know more about this.**



GOVERNMENT OF WEST BENGAL
OFFICE OF THE DISTRICT MAGISTRATE
&
COLLECTORATE
INFORMATION TECHNOLOGY
& ELECTRONICS DEPTT

Memo No: 043/IT

Date: 10/07/2017

To

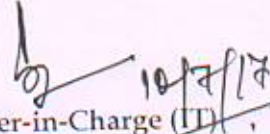
- 1-5. The Sub-Divisional Officer, All, North 24 Parganas.
- 6-27. The Block Development Officer, All, North 24 Parganas.
27. The Deputy Labour Commissioner, Barrackpore, North 24 Parganas.
- 28-31. The Assistant Labour Commissioner, Barasat/Bongaon/Basirhat/Bidhannagar, North 24 Parganas.

Sub: Action needed to prevent Petya/Petwrap ransomware-reg.

Enclose please find herewith the letter vide No: 113(70)-Com/IT/P/88/2003 Vol-V Dated: 28.6.2017 which will speak for itself regarding to ensure prevention of cyber attack and to prevent Petya/Petwrap Ransomware.

You are requested to take necessary action from your end accordingly.

Encls: as stated.

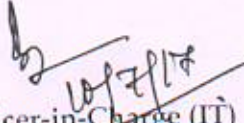

10/7/17
Officer-in-Charge (IT)
North 24 Parganas

Memo No: 043/IT/1(2)

Date: 10/07/2017

Copy forwarded for information to:

1. CA to Additional District Magistrate (General) for kind information to the Additional District Magistrate (General), North 24 Parganas.
2. The District Informatics Officer, NIC, North 24 Parganas for kind information and to upload the document regarding the above to the District Website.


10/7/17
Officer-in-Charge (IT)
North 24 Parganas