Shri Ashok K K Meena, IAS
Commissioner-cum-Secretary to Government
& Chairman, OCAC

Government of Odisha
Electronics & Information Technology Department
OCAC Building, Plot No.N-1/7-D, Acharya Vihar
Bhubaneswar-751013, Odisha, India
Ph. No.: + 91-674-2567584 (O), Fax : + 91-674-2567842
Website : www.ocac.in, e-mail : itsec.or@nic.in

Letter No. 1751 /

Bhubaneswar
Dated 16/05/2017

To

The Development Commissioner-cum-ACS
All Principal Secretaries to Government
All Commissioner-cum-Secretaries to Government
Secretary, Works Department
All Revenue Divisional Commissioner, Odisha
All Collectors

Sub: Advisory for Ransomware Threat – "WannaCry".

Madam / Sir,

As you are aware, a new Ransomware named as **"WannaCry"** is spreading wildly across the globe. WannaCry encrypts the files on infected Windows System. This Ransomware spreads by using the vulnerability in implementation of Server Message Block (SMB) in Windows System. This exploit is named as ETERNALBLUE. This Ransomware called "WannaCry" or "WannaCrypt" encrypts the computer hard disk drive and then spreading laterally between computers on the same Local Area Network (LAN). The Ransomware also spreads through malicious attachments to e-Mails.

In order to prevent infection of WannaCry, adequate steps are being taken by the Government to protect the Government data system. However, wide awareness among the Government officials and general public is essential to prevent such Cyber Attack in their computer systems. Necessary Advisory for Ransomware Threat have already been uploaded in the Odisha Government Website www.odisha.gov.in. However a copy of the advisory for Ransomware Threat is enclosed herewith for your information and wide dissemination among your subordinate offices.

Yours faithfully,

Ashok 16/5/17

Commissioner-cum-Secretary to Govt.

Dt 16.05.2017

Advisory for Ransomware Threat- "WannaCry"

(Issued by Electronics &IT Department, Government of Odisha)

1. Maintain updated Antivirus software on all systems
2. Use Genuine Software /OS for regular updates and fixes
3. In-order to prevent infection users are advised to apply patches to Windows System as mentioned in Microsoft Security Bulletin MS17 -010:https://technet.microsoft.com/library/security/MS17-010
4. Restrict users" abilities (permissions) to install and run unwanted software applications. Enable personal firewalls on workstations.
5. Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device and backups should be stored offline. At least two backups to be taken in separate media.
6. Keep the operating system's third party applications like (MSoffice, browsers, browser Plugins) up-to-date with the latest patches.
7. Do not open attachments in unsolicited e-mails, even if they come from people in your contact list and never click on a URL contained in an unsolicited e-mail even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser.
8. Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses. Block these before receiving and downloading messages. Scan all emails, attachments and downloads both on the host and at the mail gateway with a reputable antivirus solution.
9. Disable macros in Microsoft Office products. Some Office products allow for the disabling of macros that originate from outside of an organization and can provide a hybrid approach when the organization depends on the legitimate use of macros. For Windows, specific settings can block macros originating from the Internet from running.
10. Configure access controls including file, directory, and network share permissions with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories, or shares.
11. Follow safe practices when browsing the web. Ensure the web browsers are secured enough with appropriate content controls.
12. Disable remote Desktop Connections, employ least privileged accounts.

13. Use SmartScreen Filter/Malware & Phishing Filter in Internet Explorer/ Mozilla Firefox and enable Phishing and Malware Protection in Google Chrome to avoid malware & ransomware attacks.
14. Ensure use of pop blocker & ad-blockers in browsers for better security
15. Individuals or organizations are not encouraged to pay the ransom, as this does not guarantee files will be released/decrypted.
16. Block SMB ports on Enterprise Edge/perimeter network devices [UDP 137, 138 and TCP 139, 445] or Disable SMBv1. https://support.microsoft.com/en-us/help/2696547
17. Update Microsoft Patch for Unsupported Versions such as Windows XP,Vista,Server 2003, Server 2008 etc. http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598
18. Apply following signatures/rules at IDS/IPS of the Enterprise

    alert tcp $HOME_NET 445 -> any any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response"; flow:from_server,established; content:"|00 00 00 31 ff|SMB|2b 00 00 00 00 98 07 c0|"; depth:16; fast_pattern; content:"|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|"; distance:0; flowbits:isset,ETPRO.ETERNALBLUE; classtype:trojan-activity; sid:2024218; rev:2;) **(http://docs.emergingthreats.net/bin/view/Main/2024218)**

    alert smb any any -> $HOME_NET any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Request (set)"; flow:to_server,established; content:"|00 00 00 31 ff|SMB|2b 00 00 00 00 18 07 c0|"; depth:16; fast_pattern; content:"|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|"; distance:0; flowbits:set,ETPRO.ETERNALBLUE; flowbits:noalert; classtype:trojan-activity; sid:2024220; rev:1;)

    alert smb $HOME_NET any -> any any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response"; flow:from_server,established; content:"|00 00 00 31 ff|SMB|2b 00 00 00 00 98 07 c0|"; depth:16; fast_pattern; content:"|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|"; distance:0; flowbits:isset,ETPRO.ETERNALBLUE; classtype:trojan-activity; sid:2024218; rev:1;)
19. Use Private VLAN. Inter VLAN communication should be filtered/restricted.
20. Removal of “mssecsvc.exe" and "tasksche.exe" if found in the Windows Directory

---