STANDARD OPERATING PROCEDURE FOR WANNACRY ATTACK
<table>
<thead>
<tr>
<th>Document #</th>
<th>Title: STANDARD OPERATING PROCEDURE FOR HANDLING WANNACRY ATTACK</th>
<th>---</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOP-RWS-01</td>
<td>Revision # 1.0</td>
<td>Prepared By: Syam Damodaran, Rajesh.RK</td>
</tr>
<tr>
<td></td>
<td>Reviewed By: K.Anilkumar</td>
<td>Date Reviewed: 26-06-2017</td>
</tr>
<tr>
<td></td>
<td>Approved By: Governing Council</td>
<td>Date Approved: 01-07-2017</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>General Analysis on Wannacry ransomware, mitigation and prevention plans</td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Definitions</strong></td>
<td>Ransomware :- a type of malicious software designed to block access to a computer system until a sum of money is paid.</td>
<td></td>
</tr>
<tr>
<td><strong>Overview</strong></td>
<td>On May 2017, multiple companies and organizations around the world were hit by variations of a crypto-ransomware aka WannaCry / WannaCrypt / WanaCrypt0r / WCrypt / WCRY. The ransomware also acts as a worm and once it infects a system, it then self-propagates throughout the rest of the network using Eternal Blue exploit of Windows Server Message Block (SMB) protocol. The ransomware campaign caused chaos due to its massive distribution, affecting more than 150 countries and infecting over 230,000 systems. Interestingly the attack was mounted on Friday 12th May 2017, just before the weekend, making it very difficult for companies and organizations to quickly react and resolve the crisis. It targeted Windows machines including Windows XP, Windows Server 2003, Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2012 and Windows Server 2016. The &quot;payload&quot; works in the same fashion as most modern ransomwares. It finds and encrypts a range of data files and then displays a &quot;ransom note&quot; informing the user and demanding a payment in bitcoin. Once infected, the malware scans for other vulnerable system and uses the EternalBlue exploit to gain access, and the DoublePulsar tool to install and execute a copy of itself on those vulnerable machines.</td>
<td></td>
</tr>
</tbody>
</table>
| **Response Plan** | 1. Do not poweroff the infected machine as it will reduce the likelihood of successful data recovery.  
2. Isolate and disconnect the infected host from internet in order to contain the ransomware and prevent it from spreading to the rest of the network and external networks.  
3. If there are many infected machines, poweroff the router/switch to isolate and disconnect all those connected machines from internet.  
4. Analyze the extent of infection.  
5. Download a copy of wannakiwi from https://github.com/gentilkiwi/wanakiwi - Open the command prompt and run it as wannakiwi.exe ASAP as it is difficult to know how long the prime numbers used to encrypt the data will stay in the system memory before being reused by the process.  
- If that doesn’t work, find out the process id of the ransomware manually, and run the script as wannakiwi.exe [pid]. Note that the following process are to be checked for : wnry.exe, wcry.exe, data_1.exe, ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe, tasksche.exe  
- Note that this process will NOT work if the machine has been rebooted. |
Note that this will work mostly for 32 bit variants of Windows XP, Windows 2003 and Windows 7. However, has also been reported to be working in Windows Vista and Windows 2008 as well.

6. If this doesn’t work, the only way is to format the entire machine and restore a backup of the entire data.

| Prevention Plan | 1. Patch your system with Microsoft’s MS17-010 patch. This can be downloaded from [https://technet.microsoft.com/en-us/library/security/ms17-010.aspx](https://technet.microsoft.com/en-us/library/security/ms17-010.aspx). Until the patch is applied, the following two workarounds can be applied:
|               | - Disable SMBv1 with the steps documented at [https://support.microsoft.com/kb/2696547](https://support.microsoft.com/kb/2696547)
|               | - Consider adding a rule on your router or firewall to block incoming SMB traffic on port 445
|               | 2. Back-up all the essential data from your system using a 3-2-1 backup strategy.
|               | 3. Update your Antivirus/Anti malware signature database to the latest updates.
|               | 4. Install and run CCN-CERT NoMoreCry tool with the following method:
|               | - Download the tool from [https://loreto.ccn-cert.cni.es/index.php/s/tYxMah1T7x7FhND](https://loreto.ccn-cert.cni.es/index.php/s/tYxMah1T7x7FhND)
|               | - Create a shortcut of the tool
|               | - Type Win + R to open the run command and run “shell:startup”
|               | - This will open the startup folder
|               | - Paste the shortcut to this folder so that every time the machine reboots, the program runs and protects the machine.
|               | - Note that this prevention method will work for all versions of Windows.

| Best Security Practices | • Keep windows firewall turned on
|                         | • Keep your operating system and installed software always up-to date
|                         | • Backup the systems/files following the 3-2-1 scheme and verify that backups are fully operational.
|                         | • Do not open suspicious e-mails and attachments.
|                         | • Restrict access to network resources.
|                         | • Block unnecessary ports and disable unnecessary services.
|                         | • Segregate your network separating core operational systems from the rest of the network.
|                         | • Configure windows to show file extensions.
|                         | • Disable Remote Desktop Protocol.
|                         | • Keep macros disabled.
|                         | • Disable Autoplay.
|                         | • Click on links and popups responsibly.
|                         | • Install an adblocker within the browser
Appendix A

Disable SMB in Windows

1. Click on the Search option and search for “Windows Features” and you will see the result as “Turn Windows Feature on and off.”
2. Upon clicking the option, the following screen will be prompted

![Screenshot of Windows Features](image-url)
3. Now untick the box and click on “Ok”.

Disabling SMB Using PowerShell:

1. Go to Start Menu, search for PowerShell.
2. The very first result you will see is for PowerShell.
3. Right-click on the selection and select “Run as Administrator”

4. Once the PowerShell opens (with Administrator privileges)

5. Type the following command:

**Command to disable SMB v1.**

Set-Item Property -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -Value 0 –Force

**The Command to disable SMB v2**

Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB2 -Value 0 –Force

---

**Appendix B**

**Blocking ports in Windows Firewall**

1. Go to Control Panel > System and Security
4. Select Windows Firewall

3. Choose ‘Advanced Settings’
5. Select ‘Inbound Rules’ and click on ‘New Rule’

![Image of Windows Firewall with Advanced Security Interface]

6. Select Port

![Image of New Inbound Rule Wizard]

- **Rule Type**: Select the type of firewall rule to create.
- **What type of rule would you like to create?**
  - **Program**: Rule that controls connections for a program.
  - **Port**: Rule that controls connections for a TCP or UDP port.
  - **Predefined**: Custom rules
    - **BranchCache - Content Retrieval (User HTTP)**: Rule that controls connections for a Windows experience.
    - **Custom**: Custom rules
7. Select ‘Specific local ports’ and choose 445, 135

8. Select ‘Block the connection’
9. Choose default settings

10. Provide a name and description and click Finish
11. Confirm that the rule has been added.