Identifying and Reporting on Machines Vulnerable to Wanna Crypt

Background:
Due to recent events surrounding the recent outbreak of the "WannaCry" ransomware, the WannaCry/Crypt has made international headlines due to the rate of spread for a ransomware attack. The technical community is still assessing the full impact and it is important to understand the vulnerability for the attack was a known vulnerability in Windows. Those with patched OS's should not be affected.

This article is provided to assist customers during their investigation to quickly and easily create a report that identifies machines that may be at risk if they do not have the security monthly rollup or the MS17-010 patches. We have provided two options in which to generate a report, Option 1 being a report based on using log data and Option 2 based on using a custom field.

Special Note: If you have Windows XP/2003/embedded/vista machines, specific patches were released for those, and you can easily manage this through Patch Management without any further intervention. **This KB is not to be used as substitute for thorough investigation and patch strategy.**

Follow the below step-by-step instructions to generate a report based on whichever option you elect:

OPTION 1 – This generates a report using log data

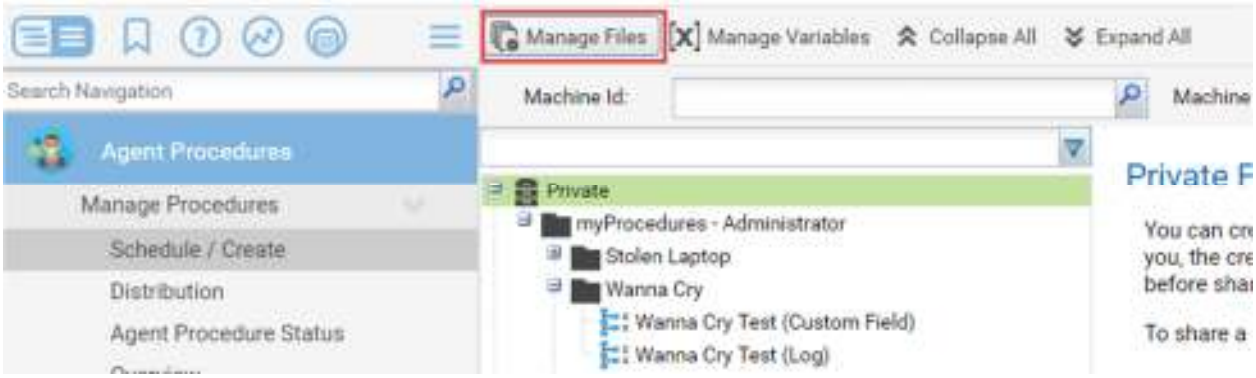
Step 1:

Decompress the zip file and find 3 attached files:

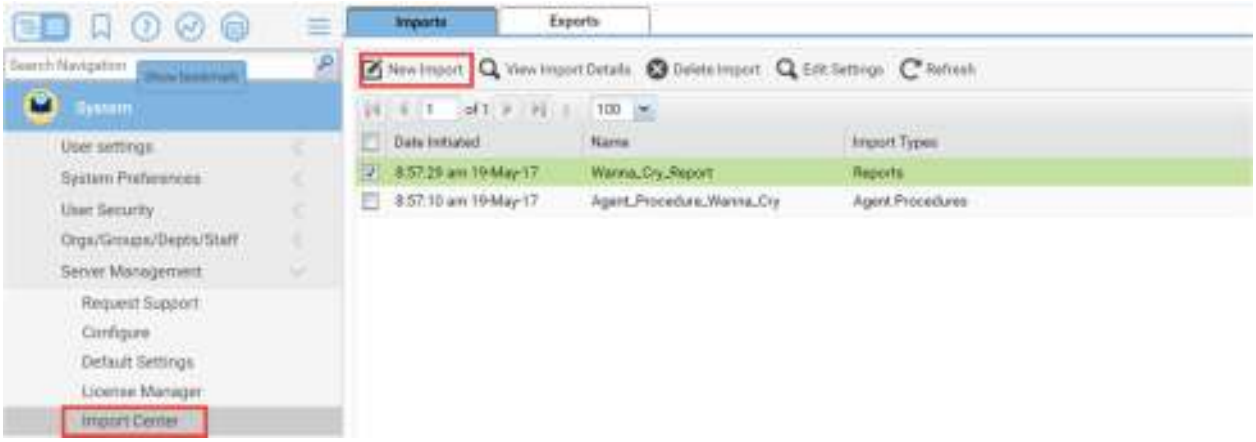
Step 2:

Upload MS17-010_Installed.ps1 in the managed files in the Agent Procedure module:

The file needs to be directly in the Shared folder.



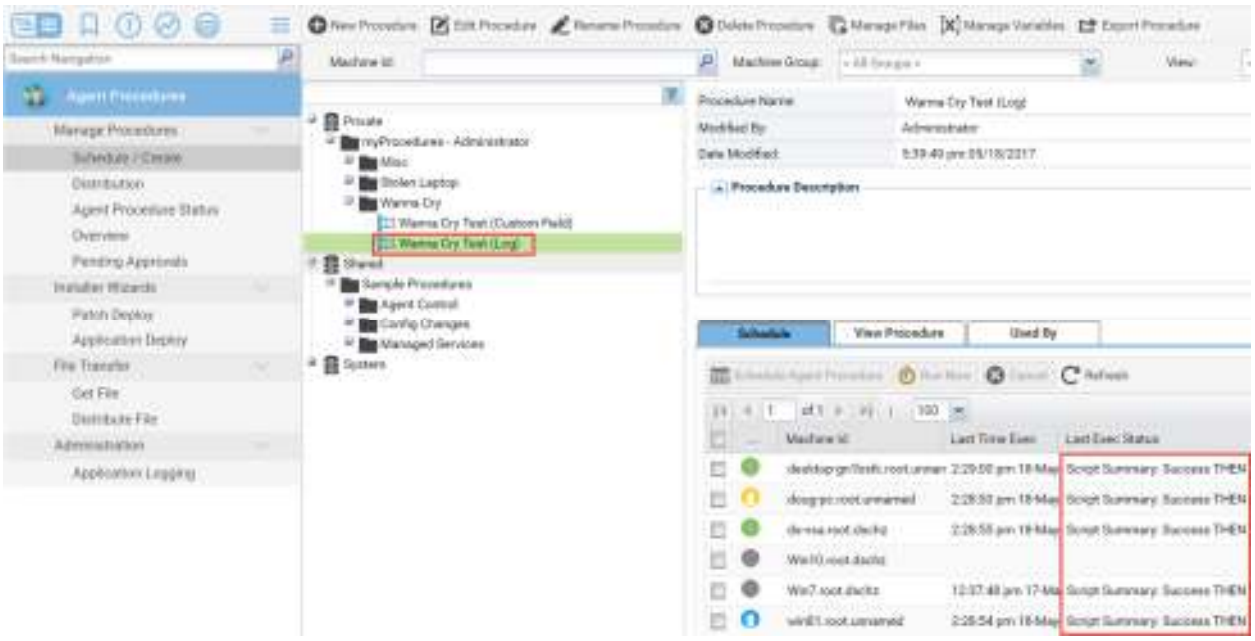
Import both XML files in the System Module under Import Center:



Step 3:

Schedule the Agent Procedure to run on all the required endpoints. (We advise no more than 50 agents at a time for a big environment, otherwise it will overload the SQL server.)

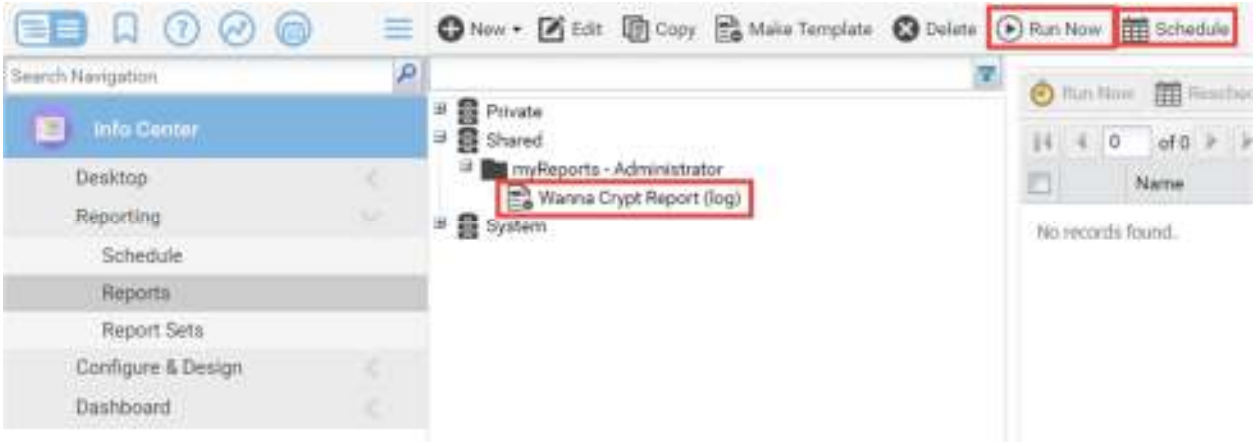
The procedure may have been imported in a different folder. The search function might be required to locate it.



Step 4:

Once the procedure has successfully ran on all agents, schedule the report in the Info Center module, under Reporting/Reports.

The Report can either be Ran Now or Scheduled at any time you need.



OPTION 2 – This generates a report using a custom field

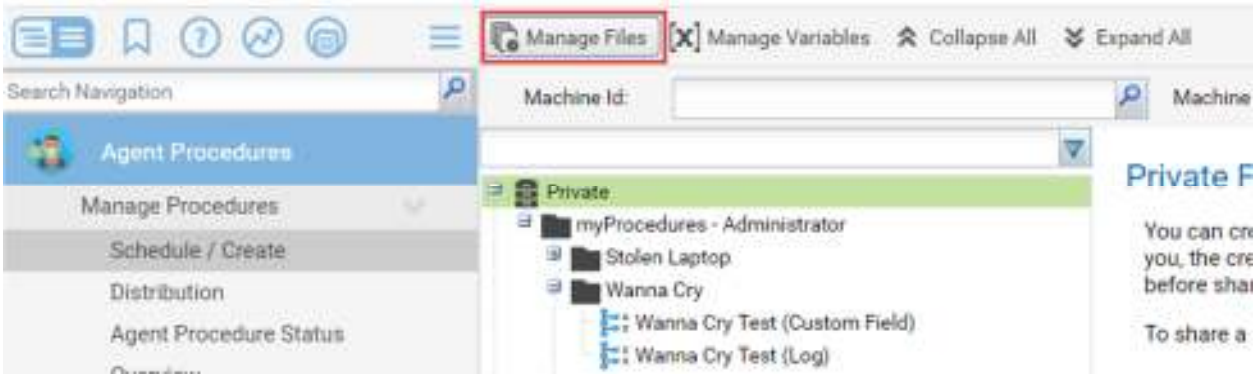
Step 1:

Decompress the zip file and find 3 attached files:

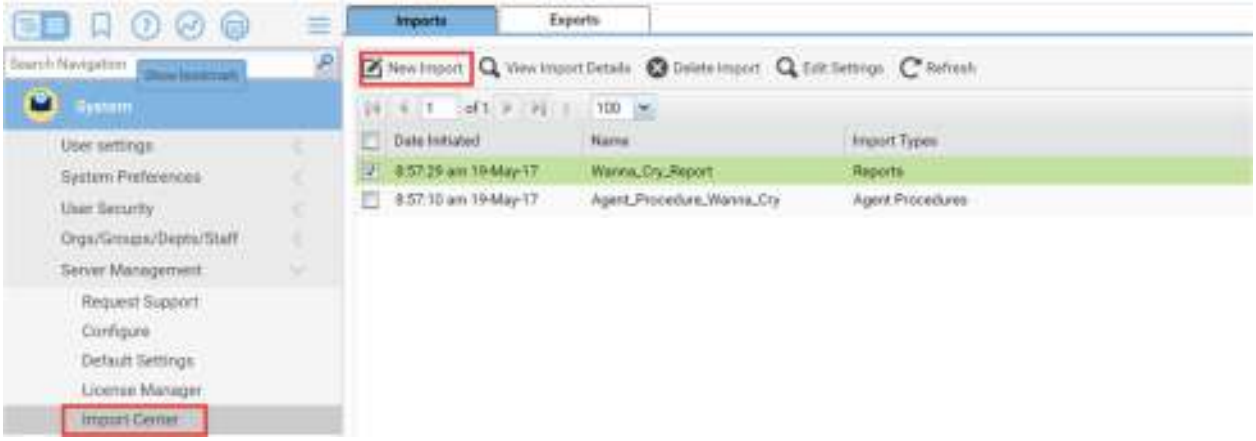
Step 2:

Upload MS17-010_Installed.ps1 in the managed files in the Agent Procedure module:

The file needs to be directly in the Shared folder.



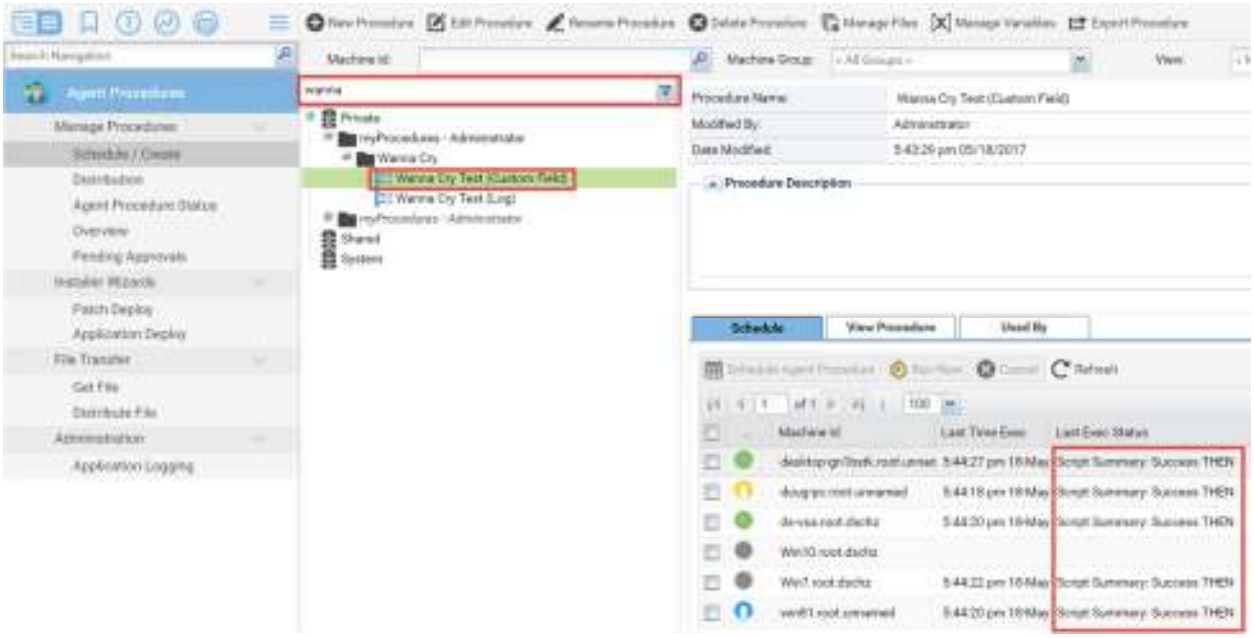
Import both XML files in the System Module under Import Center:



Step 3:

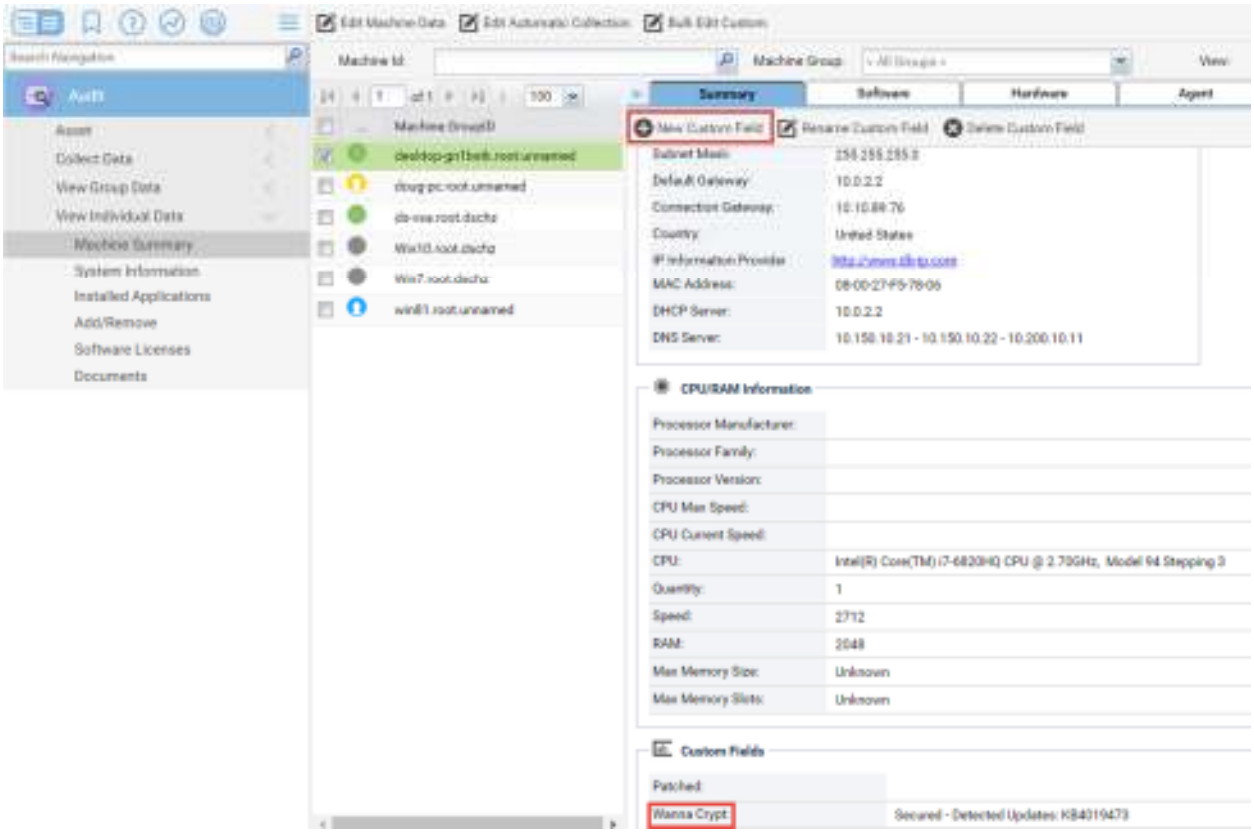
Schedule the Agent Procedure to run on all the required endpoints. (We advise no more than 50 agents at a time for a big environment, it will overload the SQL server otherwise)

The procedure may have been imported in a different folder. The search function might be required to locate it.



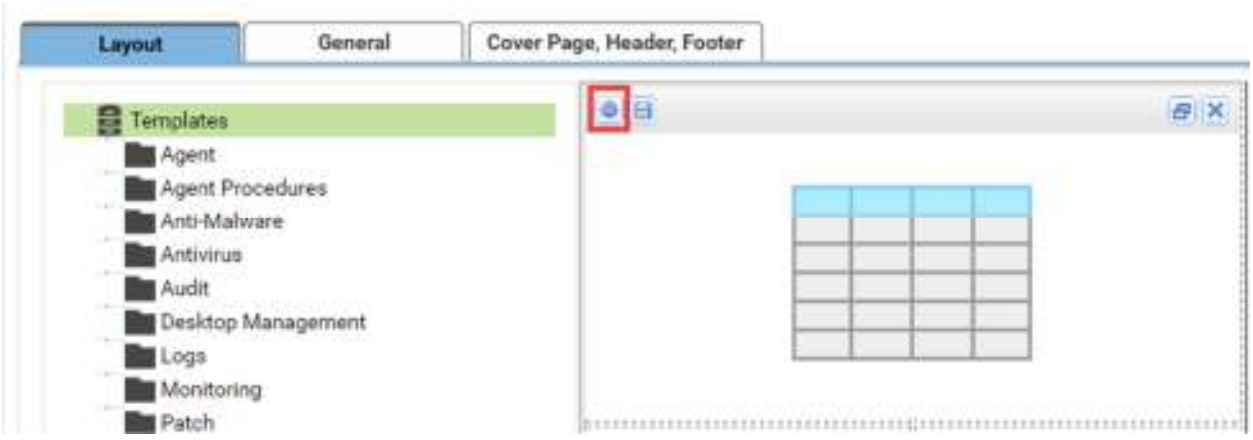
Step 4:

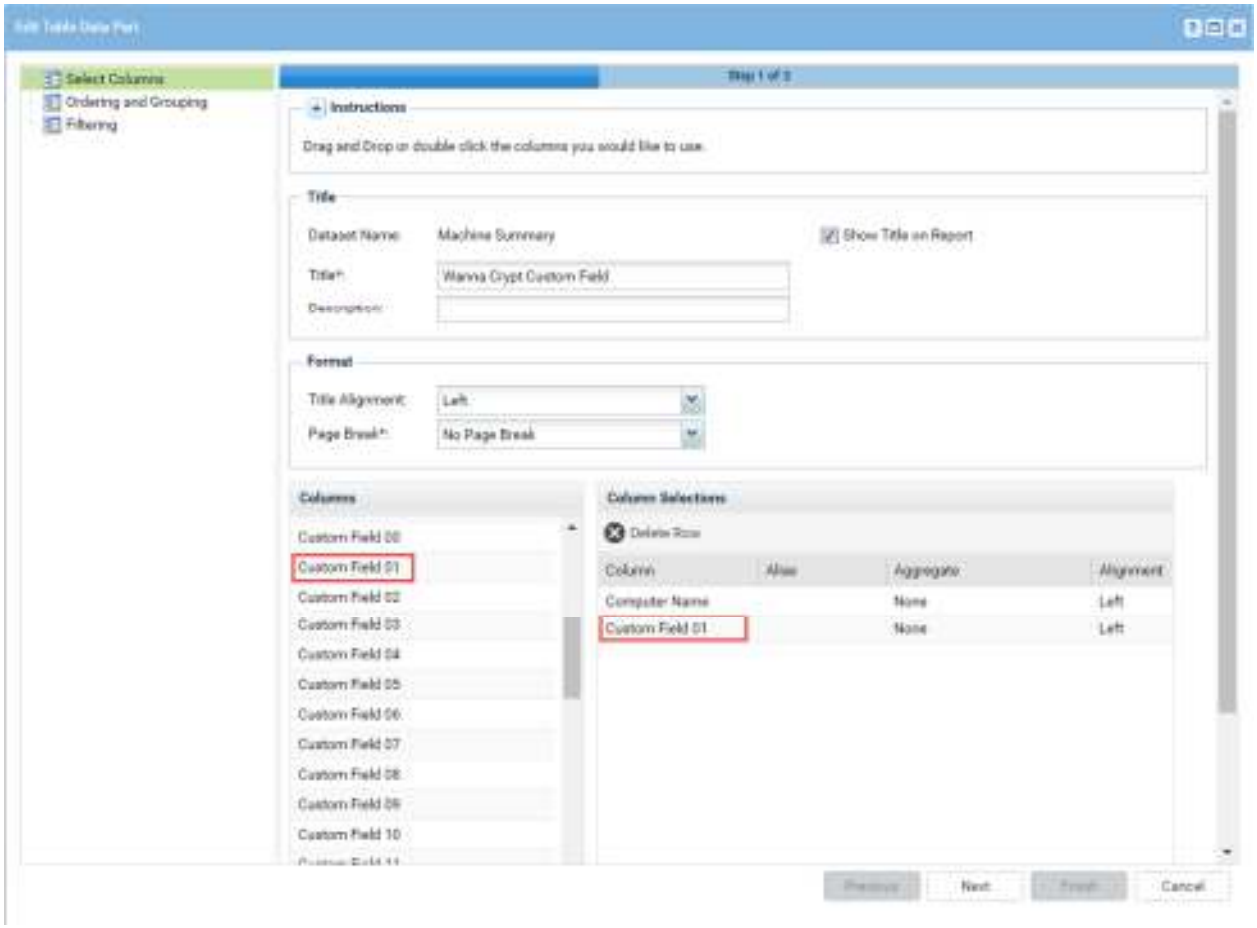
Create the Custom Field in the Audit module under View Individual Data/Machine Summary.
The Custom Field needs to be named “Wanna Crypt” for the procedure to store the data correctly.



Step 5:

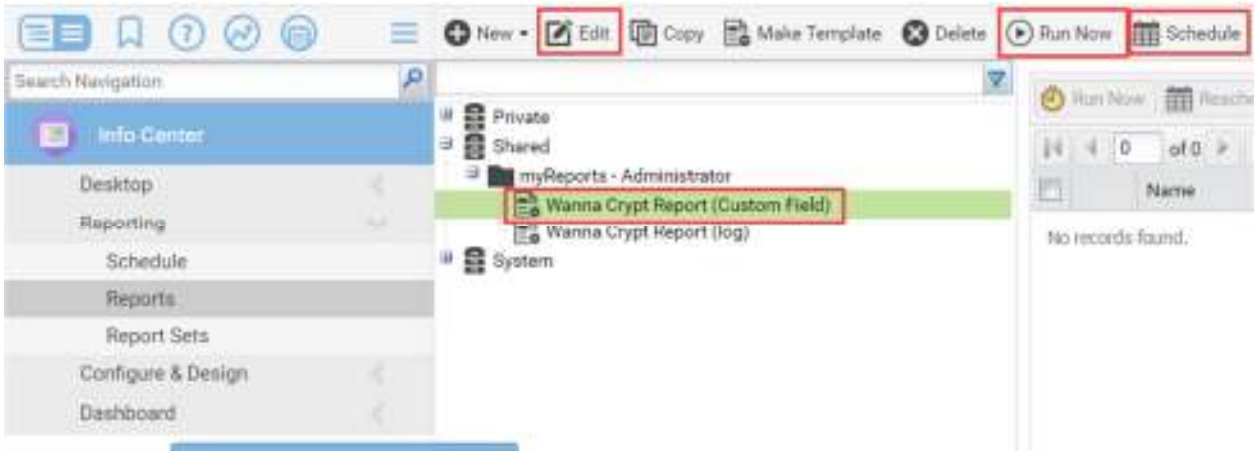
Once the procedure has been successfully ran on all agents, the report needs to be edited to display data from the correct Custom Field. In the Report module, edit the “Wanna Crypt Report (Custom Field)” to reflect the correct Custom Field. For instance, on the previous screenshot, “Wanna Crypt” is the second Custom Field being used, which in the report will show as Custom Field 01 (the first custom field starting at 00)





schedule the report in the Info Center module, under Reporting/Reports.

The Report can either be Ran Now or Scheduled at any time you need in the Info Center module, under Reporting/Reports



Step 6:

In addition to running the report, you may create a View to include all the Vulnerable machine. In any module using view, create a new View, Check the “Advanced agent data filter [Define Filter …]” Checkbox and edit the line of [Define Filter] corresponding to the Wanna Cry custom field:

The Agent Procedure would need to be ran a second time after patching the machines in order to update the data in the custom field and update the View and Report to reflect an up to date environment.

If you encounter any issues or need assistance with these steps, please contact our Kaseya Support team by submitting a support ticket via our helpdesk portal at https://helpdesk.kaseya.com/home