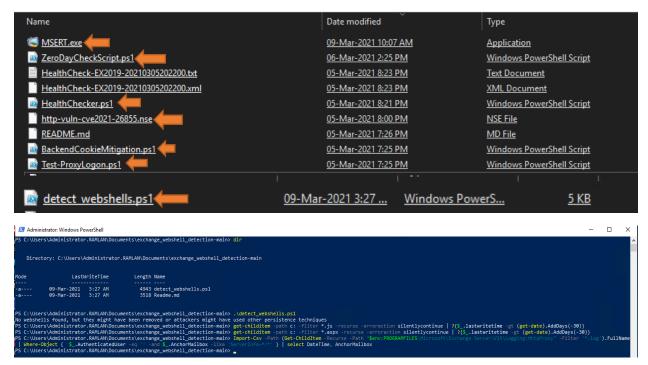
## Exchange Server 2019 Vulnerability – Exploited by Hackers – 3rd March 2021

I am running hybrid exchange 2019 within the lab. I wanted to take necessary precaution to protect mail server. I did the following to make sure the server was not compromised by the hackers.



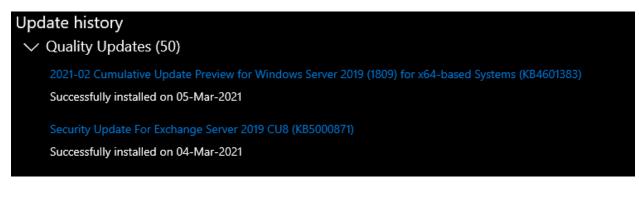
I am using various PowerShell scripts and commands to test the server. Here are the details

Import-Csv -Path (Get-ChildItem -Recurse -Path "\$env:PROGRAMFILES\Microsoft\Exchange Server\V15\Logging\HttpProxy" -Filter '\*.log').FullName | Where-Object { \$\_.AuthenticatedUser -eq '' -and \$\_.AnchorMailbox -like 'ServerInfo~\*/\*' } | select DateTime, AnchorMailbox

Get-childitem -path c: -filter \*.js -recurse -erroraction silentlycontinue | ?{\$\_.lastwritetime -gt (getdate).AddDays(-30)}

Get-childitem -path c: -filter \*.aspx -recurse -erroraction silentlycontinue | ?{\$\_.lastwritetime -gt (getdate).AddDays(-30)}

I did install these patches as well.



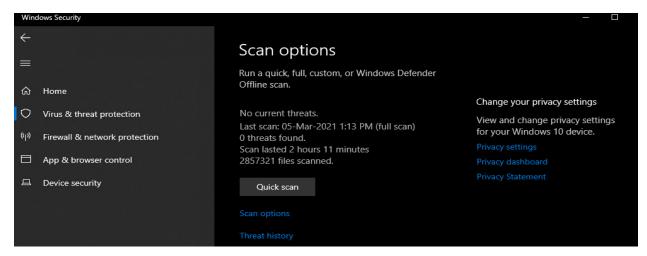
So far everything is looking good for me. I am running MSERT tool as well for extra precaution.

user license agreement You must accept the end user license agreeme	ent in order to run this tool.	· ·
Microsoft Cofety Scopper and year license are		
Microsoft Safety Scanner end user license agr	eenent.	
MICROSOFT SOFTWARE LICENSE TERMS MICROSOFT SAFETY SCANNER 1.0 These license terms are an agreement betwe where you live, one of its affiliates) and you. software named above, which includes the m The terms also apply to any Microsoft * updates, * supplements, * Internet-based services, and	. Please read them. They apply to the	
* support services	The start the second start is the second start	
for this software, unless other terms accomp apply.		
BY USING THE SOFTWARE, YOU ACCEPT TH	ESE TERMS. IF YOU DO NOT ACCEPT	~
Printable version		
Accept all terms of the preceding license ad	greement	
	<back next=""></back>	Cancel
rosoft Safety Scanner - 1.0.3001.0		
-		50
come to the Microsoft Safety Scanner This tool scans for and removes viruses, spy		
come to the Microsoft Safety Scanner This tool scans for and removes viruses, spyr software Click Next to scan for and help remove viruse	ware, and other potentially unwanted	vanted
come to the Microsoft Safety Scanner This tool scans for and removes viruses, spy software Click Next to scan for and help remove viruse	ware, and other potentially unwanted	vanted
	ware, and other potentially unwanted	vanted
Icome to the Microsoft Safety Scanner This tool scans for and removes viruses, spyr software Click Next to scan for and help remove viruse	ware, and other potentially unwanted	vanted
come to the Microsoft Safety Scanner This tool scans for and removes viruses, spyr software Click Next to scan for and help remove viruse	ware, and other potentially unwanted	vanted
Icome to the Microsoft Safety Scanner This tool scans for and removes viruses, spyr software Click Next to scan for and help remove viruse	ware, and other potentially unwanted es, spyware, and other potentially unw -malware solution. To help protect	your
Click Next to scan for and help remove viruses software	ware, and other potentially unwanted es, spyware, and other potentially unw -malware solution. To help protect	your
Click Next to scan for and help remove viruses, spyr software Click Next to scan for and help remove viruse software from your computer. This tool is not a replacement for an anti- computer, you should use an anti-malwa <u>Protect Your PC</u> .	ware, and other potentially unwanted es, spyware, and other potentially unw -malware solution. To help protect are solution. For more information,	your
Icome to the Microsoft Safety Scanner This tool scans for and removes viruses, spyr software Click Next to scan for and help remove viruse software from your computer. This tool is not a replacement for an anti- computer, you should use an anti-malwa	ware, and other potentially unwanted es, spyware, and other potentially unw -malware solution. To help protect are solution. For more information,	your
Icome to the Microsoft Safety Scanner This tool scans for and removes viruses, spyr software Click Next to scan for and help remove viruse software from your computer. This tool is not a replacement for an anti- computer, you should use an anti-malwa Protect Your PC.	ware, and other potentially unwanted es, spyware, and other potentially unw -malware solution. To help protect are solution. For more information,	your
Click Next to scan for and help remove viruses, spyr software Click Next to scan for and help remove viruse software from your computer. This tool is not a replacement for an anti- computer, you should use an anti-malwa Protect Your PC.	ware, and other potentially unwanted es, spyware, and other potentially unw -malware solution. To help protect are solution. For more information,	your
come to the Microsoft Safety Scanner This tool scans for and removes viruses, spyr software Click Next to scan for and help remove viruse software from your computer.	ware, and other potentially unwanted es, spyware, and other potentially unw -malware solution. To help protect are solution. For more information,	your

🚄 Microsoft Safety Scanner - 1.0.3001.0			×
Scan type			5
Please choose a type of scan:			
Quick scan. Scans areas of the system mo O other potentially unwanted software. If su to run a full scan.			
Full scan. Scans the entire system. Note t some computers.	hat this scan can t		l hours on
Ocustomized scan. In addition to a quick sc user-specified folder.	an, the tool will als	so scan the conte	nts of a
Choose F <u>o</u> lder			
	< <u>B</u> ack	<u>N</u> ext >	Cancel
Microsoft Safety Scanner - 1.0.3001.0			×
Full scan in progress			5
The tool is scanning your computer for viruses software.	s, spyware, and o	ther potentially ur	nwanted
After this operation completes, the tool will pr spyware, and other potentially unwanted soft			ses,
Currently scanning:			
C:\Windows\System32\ntdll.dll			
Files Scanned: 94			
Files Infected: 0			
Start time: 10:22 AM			
Time elapsed: 00:00:08			
	< <u>B</u> ack	<u>N</u> ext >	Cancel

💐 Microsoft	Safety Scanner - 1.0.3001.0 ×
Scan resu	lts
٧	The scan completed successfully and no viruses, spyware, and other potentially unwanted software were detected.
	If you continue to experience issues, please ask the <u>community</u> or submit a <u>support case</u> .
	< Back Finish Cancel

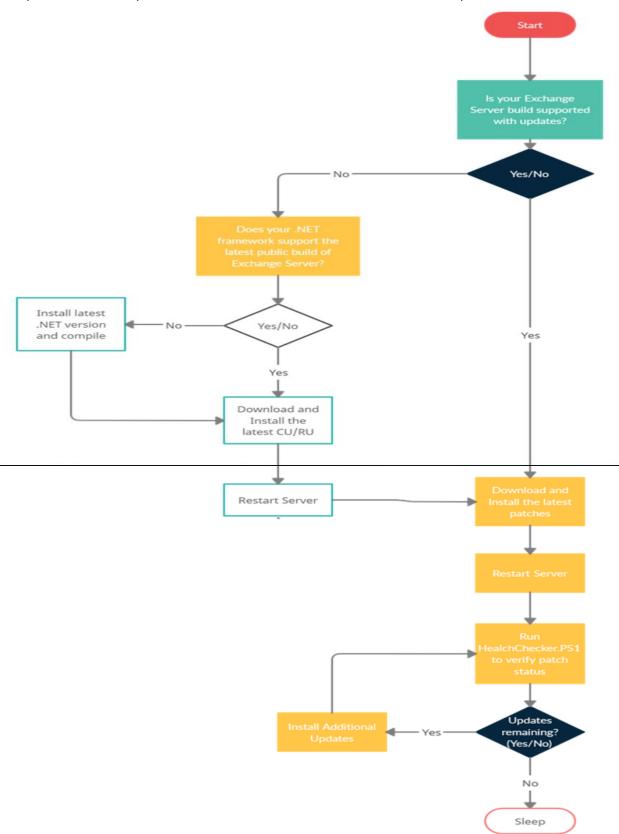
I also performed full scan using Windows Defender for extra protection.



Now, I am happy the mail server is not compromised and hackers did not penetrate the mail server.

Thanks

Ram Lan 9<sup>th</sup> Mar 2021



This picture below, I copied from Microsoft site for eash reference on how to protect mail server.