The Microsoft MSERT tool can find web shells related to the Exchange Server attack campaign

Microsoft has just released a new update to MSERT, which comes with the ability to detect web shells deployed in recent Exchange Server attacks.

Earlier on March 2, Microsoft publicly disclosed that up to four Exchange Server zero-day vulnerabilities were being abused in a large-scale attack against Outlook servers on the web (Outlook on the web. - OWA) was revealed. These four vulnerabilities are currently being tracked with identifiers CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065, respectively.

Known as 'ProxyLogon', these flaws are being thoroughly exploited by Chinese-sponsored hacker groups to steal email messages, collect login credentials, and deploy web shells for access. access to a wide range of targeted intranet systems.

In making this offensive campaign public announcement, Microsoft also released updated signatures for Microsoft Defender to add the ability to detect unauthorized installed web shells by abusing zero vulnerabilities. -day above.

These web shells are detected by Microsoft Defender with the following specific information:

1. Exploit: Script / Exmann.A! Dha
2. Behavior: Win32 / Exmann.A
3. Backdoor: ASP / SecChecker.A
4. Backdoor: JS / Webshell
5. Trojan: JS / Chopper! Dha
6. Behavior: Win32 / DumpLsass.A! Attk
7. Backdoor: HTML / TwoFaceVar.B

For organizations that don't use Microsoft Defender, the Redmond company has added update signatures to their Microsoft Safety Scanner stand-alone tool to add the ability to find and remove web shells used in hacking campaigns. this work.

Microsoft Safety Scanner helps to remove web shell

Microsoft Safety Scanner, also known as Microsoft Emergency Response Assistant (MSERT), is a portable standalone anti-software tool that includes a Microsoft Defender signature to scan and remove detected malware .

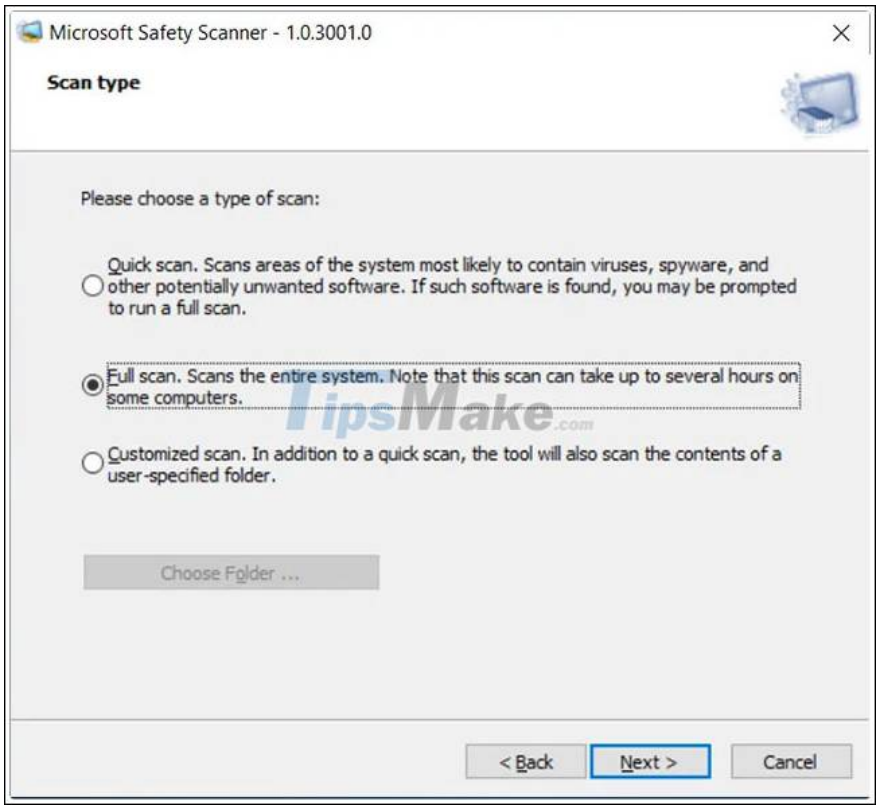
MSERT can be considered as an on-demand scanner and will not provide any real-time protection. Therefore, this tool should only be used for spot scanning and should not be considered as a standalone antivirus program.

Furthermore, MSERT will also automatically delete any detected files and not quarantine them if you don't start the program with the / N argument, as in msert.exe / N. To scan web shells and not delete them, you can also use the PowerShell script described at the end of the article.

The Microsoft Safety Scanner can be downloaded as a 32-bit or 64-bit executable and used to perform on-site scans when needed.

After launching the program, agree to the license agreements and you will be taken to a screen to choose a scan type.

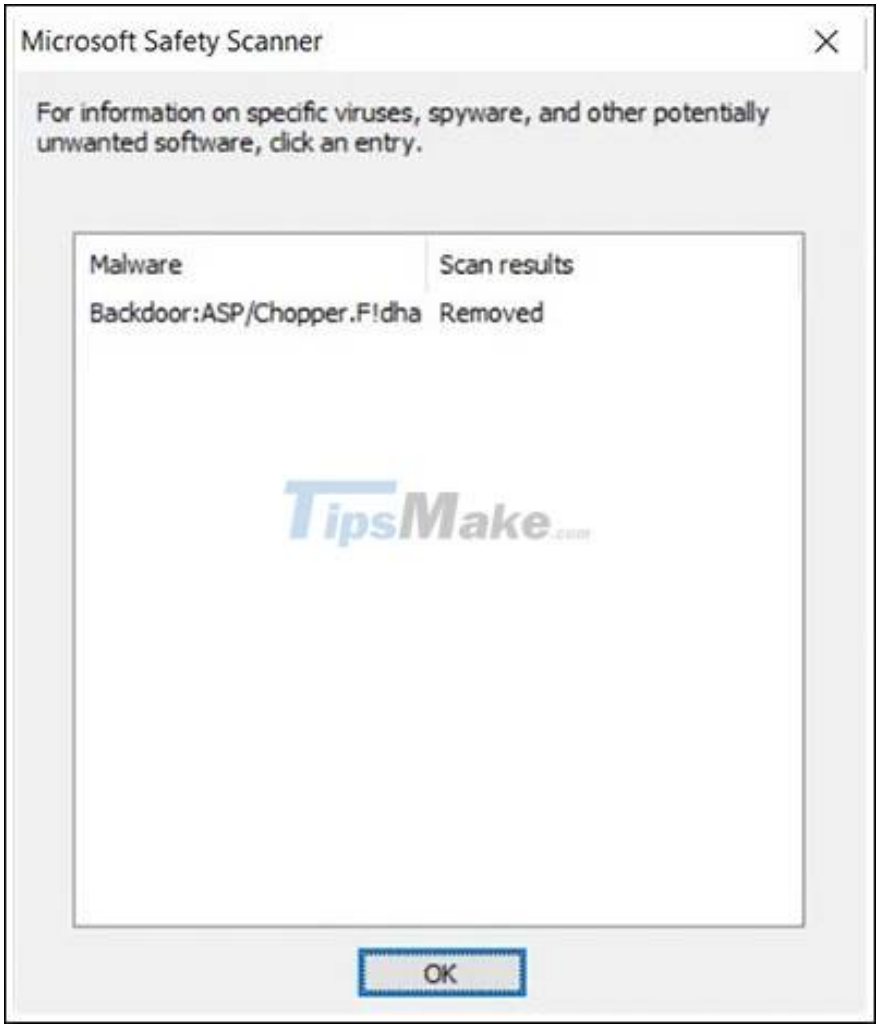
Microsoft generally recommends that users choose the 'Full scan' option to scan the entire server.



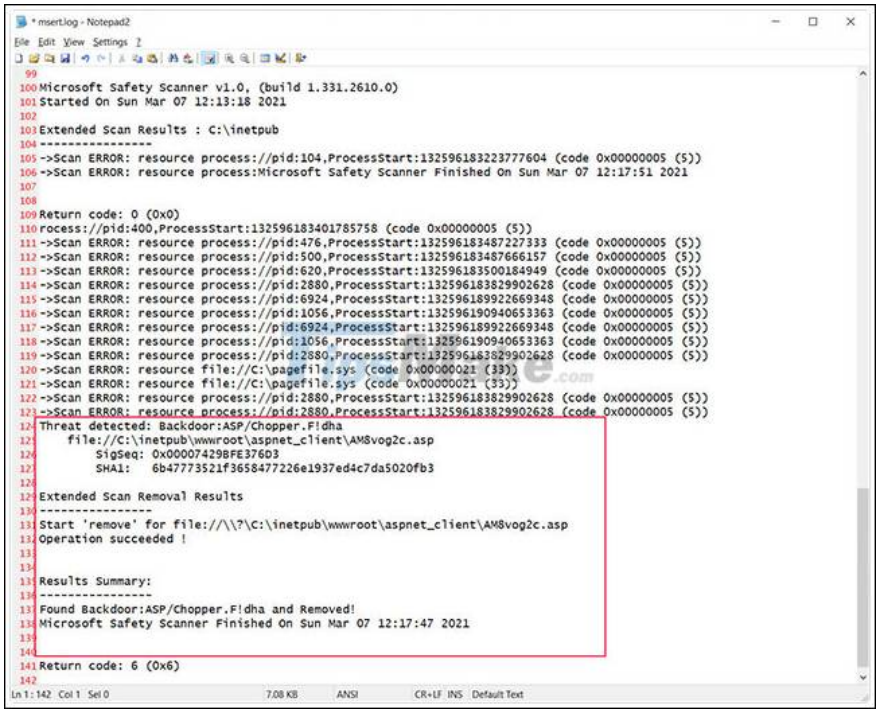
Depending on the size of your installation, the full scan might take quite a while. Therefore, you can perform a 'Customized scan' of each important folder, such as:

1. % IIS installation path% aspnet_client *
2. % IIS installation path% aspnet_clientsystem_web *
3. % Exchange Server installation path% FrontEndHttpProxyowaauth *
4. Configured temporary ASP.NET files path
5. % Exchange Server Installation% FrontEndHttpProxyecpauth *

After the scan is finished, MSERT will report which files have been deleted and their specific names.



For more detailed information on which files have been deleted, you can refer to the file% SYSTEMROOT% debugmsert.log, as shown below.

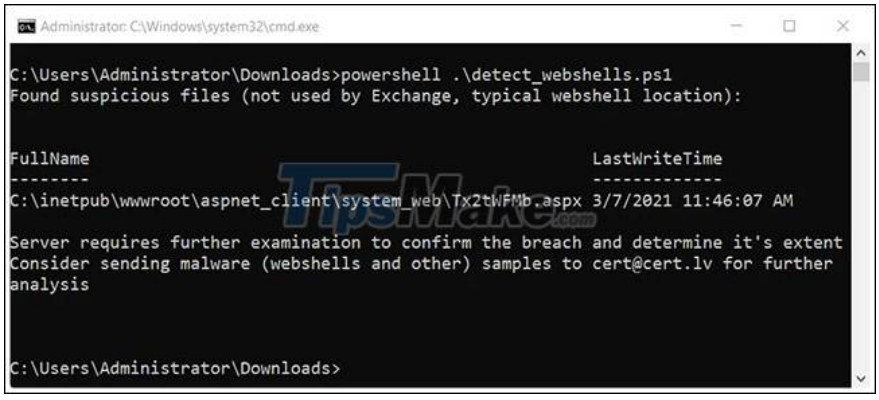


Once you're done using MSERT, you can uninstall the tool by deleting the executable msert.exe.

PowerShell scripts support finding web shells

If you want to scan web shells without deleting them, you can use a new PowerShell script called detector_webshells.ps1 created by Latvian CERT.

This script will display files containing specific strings used by web shell, but not Microsoft Exchange, in ProxyLogon attacks. The advantage of detector_webshells.ps is that it will not delete the file and facilitate further analysis later.



You can find more information on how to use this script in the CERT-LV project's GitHub repository.

In addition, Microsoft has just released a PowerShell script called Test-ProxyLogon.ps1, which can be used to look for intrusion index (IOC) related to ProxyLogon attacks in log files. Exchange and OWA.

You finished reading the article "**The Microsoft MSERT tool can find web shells related to the Exchange Server attack campaign**" edited by the **TipsMake** team. We hope this article has provided you with many

useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.