SENT 03-06-2021.
ATTACHMENTS: 0

Urgent and Critical New Information Released Concerning Microsoft Exchange Exploit

If you are receiving this email, you are among the clients whose Microsoft Exchange Servers we applied an emergency Microsoft patch to this week.

Although Microsoft only announced the discovery of the recently patched security flaw a few short days ago, we have since been following discussion forums concerning the matter. Two new facts have now come to light that give us great cause for concern:

1. The flaw may have been in existence as early as January of this year.

2. Because the malicious actors utilized automated methods to deploy backdoor software to targeted servers, the number of servers actually affected is significantly greater than what was initially conveyed to the public.

For this reason, we are proactively running a script just released by Microsoft to help identify servers that were infected with the backdoor, in addition to performing other malware scans and manual inspections.

If evidence of the backdoor having been installed is found on your Exchange server, we will reach out to you individually right away.

Question: What if we find evidence of the backdoor having already been deployed to your server prior to the Microsoft patch being applied?

First, it is important to understand that although the backdoor may have been deployed to your server, it does NOT necessarily mean that the malicious actors have actually connected to your server and exfiltrated data. It only means that the backdoor was deployed.

That said, our recommendation is to err on the side of caution if the backdoor is found on your server.

That means immediately disabling Microsoft Exchange to prevent potential access. After that, we recommend creating a forensic image of your server, removing the exploit, changing all passwords, then restoring service.

The foregoing course of action is of course subject to your individual discretion. If it is your desire to have your server thoroughly examined for any evidence that malicious actors actually connected to your server and exfiltrated data, making a forensic image prior to taking actions to remove the backdoor is essential. If you do not wish to have your server examined for this purpose, the backdoor can be removed without first making a forensic image.

Our professional recommendation is the former, however the choice is one that must be made by the business owner(s) and their legal representatives, it is NOT a choice that can be made by our firm.

Due to the number of Exchange servers in deployment within our client base, we will be scanning servers throughout the weekend. **If the backdoor is found on your Exchange server, you will be contacted for approval to proceed with one of the two courses of action described above.**

Given the widespread nature of this problem that has now come to light, you may wish to consider what actions you would like taken in advance, in case we find the backdoor to have been deployed to your server.

If you have any questions, please feel free to reply to this email and we will respond as promptly as possible.

Aaron Arlotti
Manager, Remote Support Operations
Sandbox Technologies, Inc