Ransomware targeting Adobe CF 9 - September 2021

Background about the situation:

In September 2021, a group started to use a combination of CF 9 exploits to install ransomware on servers. Sophos has an article about the exploit and ransomware they saw on a ColdFusion 9 server running on Windows Server 2008. However, it is possible that other variations of this are happening and could affect other OS or possibly use other exploits on different versions of Adobe ColdFusion.

The Sophos Article can be found here: https://news.sophos.com/en-us/2021/09/21/cring-ransomware-group-exploits-ancient-coldfusion-server/

- This is a good article to read and gives an understanding on what looks to be happening from the data they were able to see.

Recommendations:

- We recommend at a minimum that you lock down your CF Administrator to localhost or other known specific IP address. Please see ColdFusion IP Lockdown
    - For full lockdown of your CF install, you can review the full guides on this page: Adobe ColdFusion Lockdown Guides
- Review your server and look for any of the mentioned exploited files that were seen in the Sophos article
- If you have Sophos Endpoint protection or other A/V or Ransomware protection on your server, ensure that tamper protection is turned on.
- For clients that have "Sophos Server Protection" as part of your hosting from Vivio, Sophos is converting clients to a new version called "Intercept X Essentials for Server." This version has some basic Ransomware protection added, and Sophos is removing some functions from the "Sophos Server Protection" edition. All clients will be starting to get converted in the next few months. But it looks like we can manually update to the new version now on your current install. Please e-mail support@viviotech.net if you would like us to go and manually update you to the new version.
    - We recommend either getting "Intercept X Essentials for Server", "Sophos Intercept X Advanced for Server" or higher level version of Sophos endpoint to help protect against the ransomware if you currently do not have any Ransomware protection.
    - You can review this pdf of the feature sets of the different versions: https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/Server_protection_licensing_guide-na.pdf

Server_protectio...na-Sept-2021.pdf

If you would like help with implementing any of the above recommendations, please get in touch with our Support team.