

RANSOMWARE **ALERT!**

Server Edition

SHUTDOWN ALERT!

Alert tells you a ransomware attack was detected against the server! Please save your work. This workstation will shutdown in two minutes!

You're about to be signed out

This is an automated message from CryptoStopper: This machine has been compromised by Ransomware. The computer will shut down in 2 minutes. Please save your work!!! An administrator has already been notified.

Close

Expires 9/2/2021

Restoring Network Connections

NOTIFIC

An error occurred while reconnecting Z: to \\ch-2k16fs-lab\TestData2 Microsoft Windows Network: The local device name is already in use.

This connection has not been restored.

ISOLATE FROM SHARE

The infected workstation is isolated from the server share stopping the ransomware attack

Email alert notifies admin that attack has occured and has been stopped before the admin was aware an attack took place





EMAIL Think before you click!

×

OK

estco Products Server CH-2K16F5-IAB detected a remote ransomware attack from user demowpd on 192.168.15.12 at Time: 9/2/2020 11:16:44 AM. A potentially mail ackup.mp4 Please check the host immediately.



REMEDIATE

Clean the workstation of malware or reimage the workstation before putting back on the LAN

BACK TO WORK

Remove workstation from isolation to resume access to share

- Open Windows Firewall
- Select Inbound Rule
- Select Canauri
- Click Scope Tab
- Remove Isolated IP address
- Click Apply

