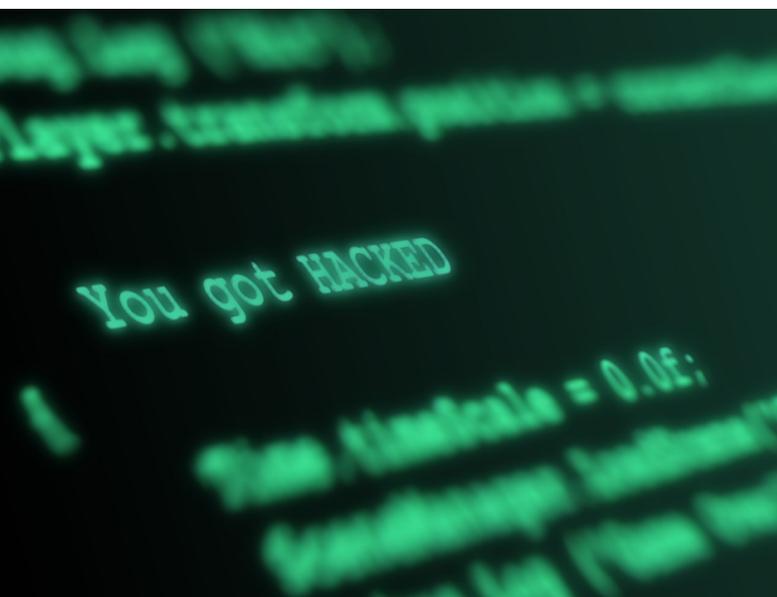


PROTECT YOURSELF FROM RANSOMWARE

STAGES OF RANSOMWARE INFECTION :



STEP 1:

DELIVERY

The network is compromised by a phishing email, exploit or worm.

STEP 2:

COMMAND & CONTROL

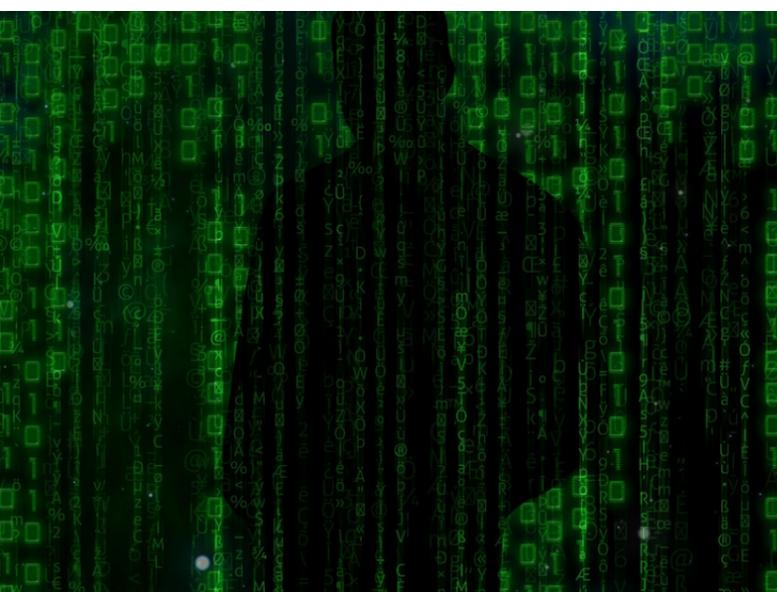
Once inside network, the ransomware establishes a connection with the attacker's command and control server to receive instructions. Still undetected, the malware continues to set the stage for its attack by stealing credentials and gaining access to more accounts across the network.



STEP 3:

ENCRYPTION & EXTORTION

The virus searches for files to encrypt—both on the local workstation and on any networks it has gained access to through lateral movement. Cybercriminals begin to exfiltrate and/or encrypt local and network files. The attacker demands payment to have them decrypted or released back to the business.



STAY CYBER SAFE



Regularly backup data & keep them offline



Keep your Antivirus up-to-date



Disable ActiveX content in MS Office applications



Do not click on links or download attachments in unsolicited emails



Keep OS & applications up-to-date with latest patches

FOR MORE CYBER SECURITY TIPS :

VISIT https://canarabank.com/User_page.aspx?othlink=356

OR Scan QR Code:

