A CYBERCRIME TOOL TO GAIN UNLIMITED ACCESS TO YOUR COMPUTER

Once installed, a RAT will allow cybercriminals to watch and listen through the camera and microphone, record all your on-screen activity, alter your personal files and use your device to distribute malware to other computers.

BE AWARE OF THE RAT – INFECTION SIGNS

- Your internet connection is unusually slow
- Your files are modified or deleted without your permission
- Unknown processes are running in your system (visible in the Task Manager, Processes tab)
- Unknown programs are installed on your device (visible in the Control Panel, Add or Remove Programs)

PROTECT YOURSELF

- Ensure that your security software and operating system are up to date
- Ensure that your device’s firewall (if available) is active
- Only download apps and software from sources you can trust
- Cover your webcam when not in use
- Regularly back-up your data
- Be wary while browsing the internet and do not click on suspicious links, pop ups or dialogue boxes
- Keep your web browser up to date and configured to alert you whenever a new window is opened or anything is downloaded
- Do not click on links or attachments within unexpected or suspicious emails

INFECTED? WHAT TO DO NEXT

- Disconnect your device from the network as soon as possible, in order to prevent additional malicious activity
- Install security software from a trustworthy source
- Run a full scan of your device and remove the threats by using security software
- Once you think that the infection has been removed, change the passwords for your online accounts and check your banking activity. Report anything unusual to your bank and, as needed, to your local law enforcement authorities
- Learn how to protect your computer from future infections and avoid data loss