|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Group : 6 Roll No.** | **41,42,43,44,45,46,47,48** | | | |
| **Name of Microproject** | **Ransomware** | | | |
| **Details of Student(s)** | **Enrollment #** | **Exam Seat #** | **Name of Student(s)** | |
| 1910020360 | 440121 | Raut Atharva Satish | |
| 1910020361 | 440122 | Sanap Yash Dilip | |
| 1910020362 | 440123 | Savant Omkar Vitthal | |
| 1910020363 | 440124 | Sawant Diksha Pravin | |
| 1910020364 | 440125 | Shimpi Om Vilas | |
| 1910020365 | 440126 | Solase Sushant Ashok | |
| 1910020366 | 440127 | Sonar Yashoda Ranbir | |
| 1910020367 | 440128 | Sonawane Isha Balasaheb | |
| **Project Guide(s)** | Prof. P. N. Patil | | | |
| **Name of Industry** | NA | | | |
| **Nature of Project** | Application Base | | | |
| **Application(s) of Project** | Software Industry | | | |
| **Abstract**: Starting from around 2012 the use of ransomware scams has grown internationally. There were 181.5 million ransomware attacks in the first six months of 2018. This marks a 229% increase over this same time frame in 2017. In June 2014, vendor McAfee released data showing that it had collected more than double the number of samples of ransomware that quarter than it had in the same quarter of the previous year. | | | | |
| **Introduction**: Ransomware is a type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. In a properly implemented cryptoviral extortion attack, recovering the files without the decryption key is an intractable problem – and difficult to trace digital currencies such as Ukash or Bitcoin and other cryptocurrency are used for the ransoms, making tracing and prosecuting the perpetrators difficult. ansomware attacks are typically carried out using a Trojan that is disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment. However, one high-profile example, the "WannaCry worm", travelled automatically between computers without user interaction. | | | | |
| HTML - Wikipedia | A screenshot of text  Description automatically generated | | | A screenshot of a social media post  Description automatically generated |
| **Fig. 1: HTML 5** | **Fig. 2: Source Code** | | | **Fig. 3: Output** |
| **Competitions**: NA | | | | |