RANSOMWARE ATTACK TOOLS AND TECHNIQUES

Sahibjot Singh Aneja

(Intern at Gurugram Police Cyber Security Summer Internship)

So what is a ransomware?

- Ransomware is a malware which encrypts files ,which are meant to be encrypted ,on victims system.
- The attacker asks for a heavy ransom(money) from the victim in order to give him decryption key.

How do these ransomware get into your system?

- Before understanding techniques to protect ourselves from ransomware, we need to know how this malware gets into your system and steps which are followed to encrypt files.
- Almost all major hacks and cybercrimes today happen by fooling people, so does these ransomwares.
- **Ways by which this malware infect our system:**

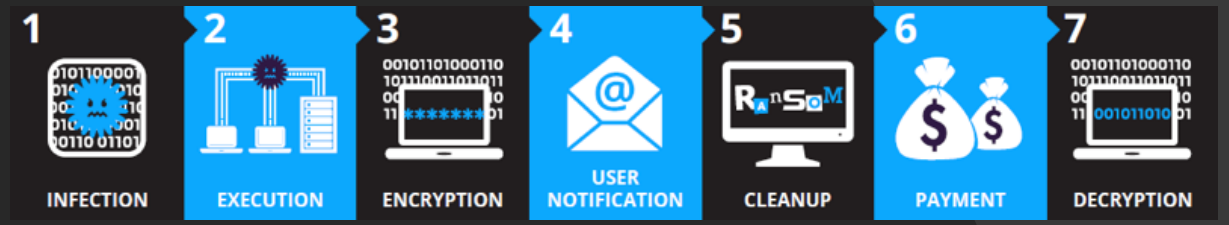
I. Due to malicious links in body of e-mail.

II. Download malicious files attached to emails like RAT'S, spyware etc.

III. Clicking malicious advertisements on websites (even trusted websites can be compromised by injecting JS code)

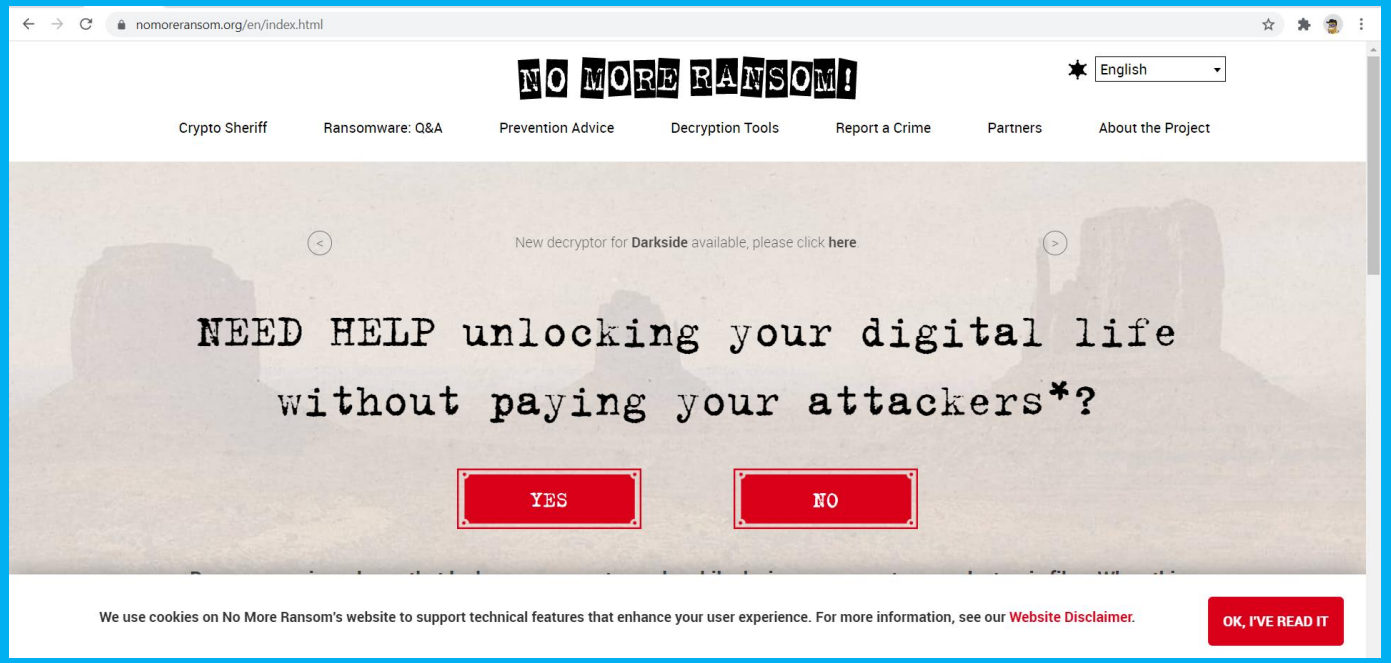
How does ransomware effects system?

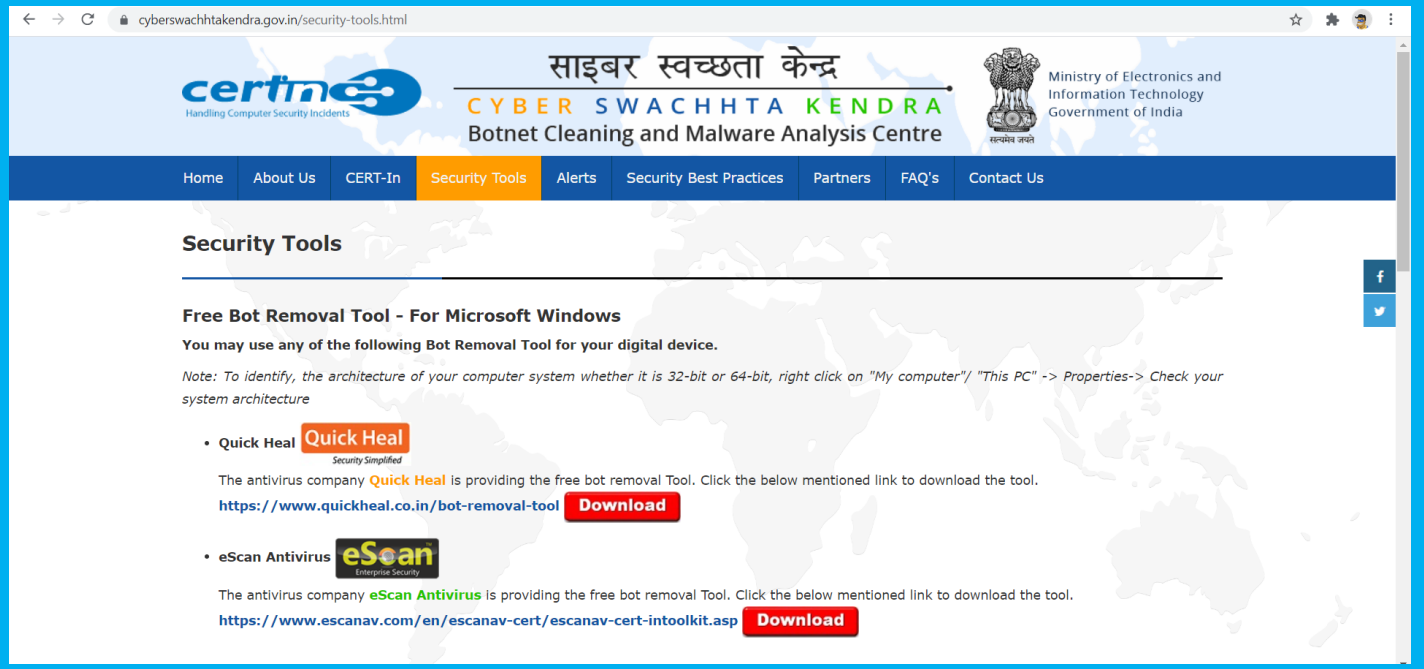
- Ransomware exploits some specific vulnerability in the system and encrypt all files that it is meant to encrypt.
- This process takes place in steps.
- First **INFECTION** takes place i.e. malware is downloaded in the system.
- Then in **EXECUTION** step the malware searches for all files that it is programmed to encrypt.
- Then comes **ENCRYPTION** phase in which files are encrypted.
- Then a message dialog box appears on victim's screen asking for money.
- Then **CLEANUP** occurs in which ransomware deletes itself.
- Attacker asks victim to do payment on dark web using bitcoins so that attacker remains anonymous.
- Then attacker sends decryption key to victim though in many cases attacker doesn't send it even after getting money.



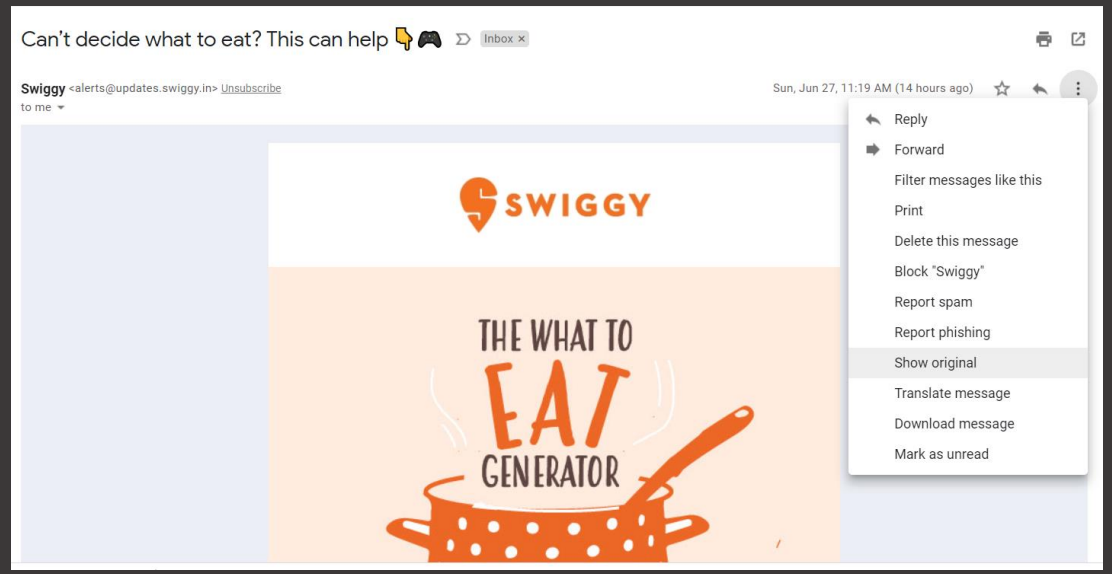
TECHNIQUES

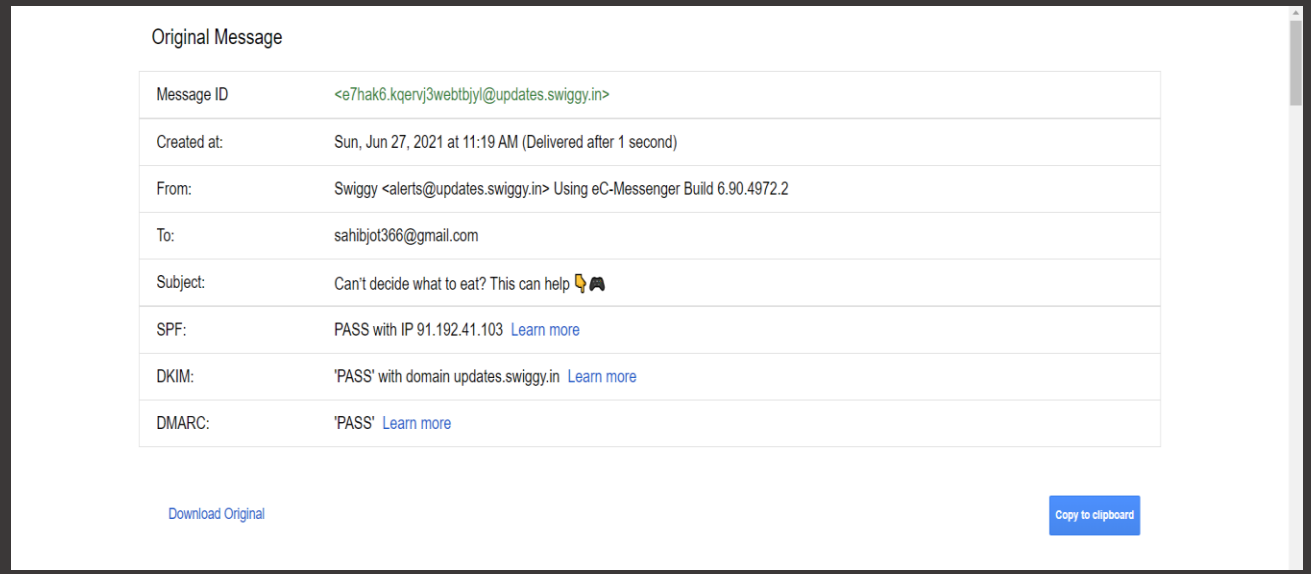
- Many government agencies and cybersecurity companies tied up and built a platform called **nomoreransom.org (**https://www.nomoreransom.org/) This is brilliant platform where decryption keys of many known ransomwares is available.
- Indian government has also provided such platforms like https://www.cyberswachhtakendra.gov.in/
- Always Keep your Operating system updated as Ransomwares exploit vulnerabilities in system. These vulnerabilities can easily be exploited in a system which is not up to date.
- Also install a paid antivirus software in your system (although it is not much effective against newly made ransomwares as they work on basis of signatures of known malwares).
- Regularly take 2-3 backups of all your important files and keep it in separate place.


nomoreransom.org/en/index.html
NO MORE RANSOM!
English
Crypto Sheriff
Ransomware: Q&A
Prevention Advice
Decryption Tools
Report a Crime
Partners
About the Project
New decryptor for Darkside available, please click here
NEED HELP unlocking your digital life without paying your attackers*?
YES
NO
We use cookies on No More Ransom's website to support technical features that enhance your user experience. For more information, see our Website Disclaimer.
OK, I'VE READ IT

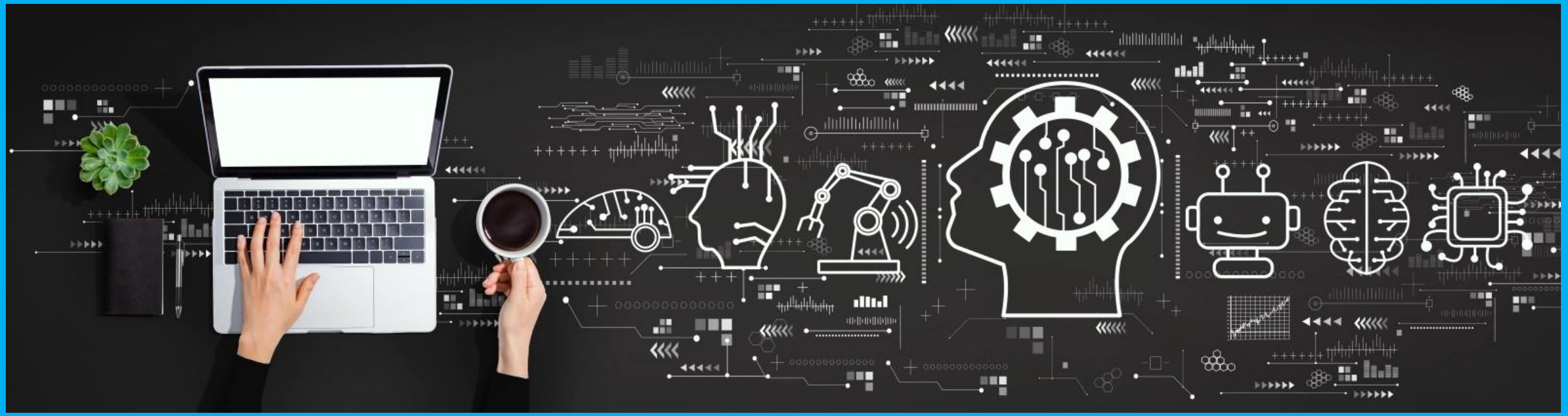

cyberswachhtakendra.gov.in/security-tools.html
certin
Handling Computer Security Incidents
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
Ministry of Electronics and Information Technology
Government of India
Home
About Us
CERT-In
Security Tools
Alerts
Security Best Practices
Partners
FAQ's
Contact Us
Security Tools
Free Bot Removal Tool - For Microsoft Windows
You may use any of the following Bot Removal Tool for your digital device.
Note: To identify, the architecture of your computer system whether it is 32-bit or 64-bit, right click on "My computer"/ "This PC" -> Properties-> Check your system architecture
Quick Heal
Quick Heal
Security Simplified
The antivirus company Quick Heal is providing the free bot removal Tool. Click the below mentioned link to download the tool.
https://www.quickheal.co.in/bot-removal-tool
Download
eScan Antivirus
eScan
Enterprise Security
The antivirus company eScan Antivirus is providing the free bot removal Tool. Click the below mentioned link to download the tool.
https://www.escanav.com/en/escanav-cert/escanav-cert-intoolkit.asp
Download

- You should be very careful while clicking any link on email, social media and websites. There is an option SHOW ORIGINAL(in g-mail) or VIEW RAW MESSAGE(in yahoo). Check header of e-mail. If valid then only trust that mail.
- Never open or download suspicious e-mail attachments.
- Never use unknown pen-drives.



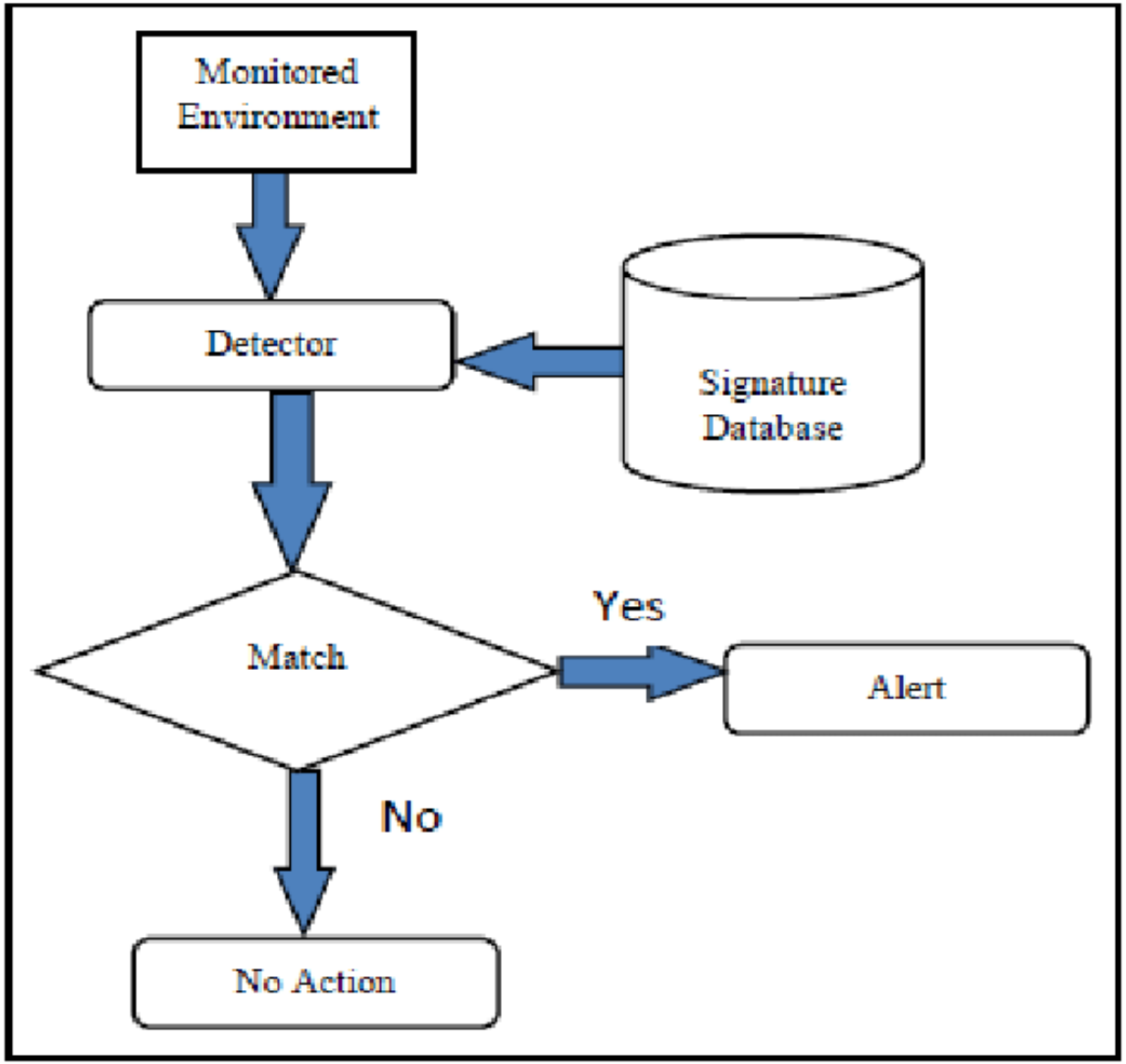


MACHINE LEARNING:
BEST TECHNIQUE AGAINST RANSOMWARES.



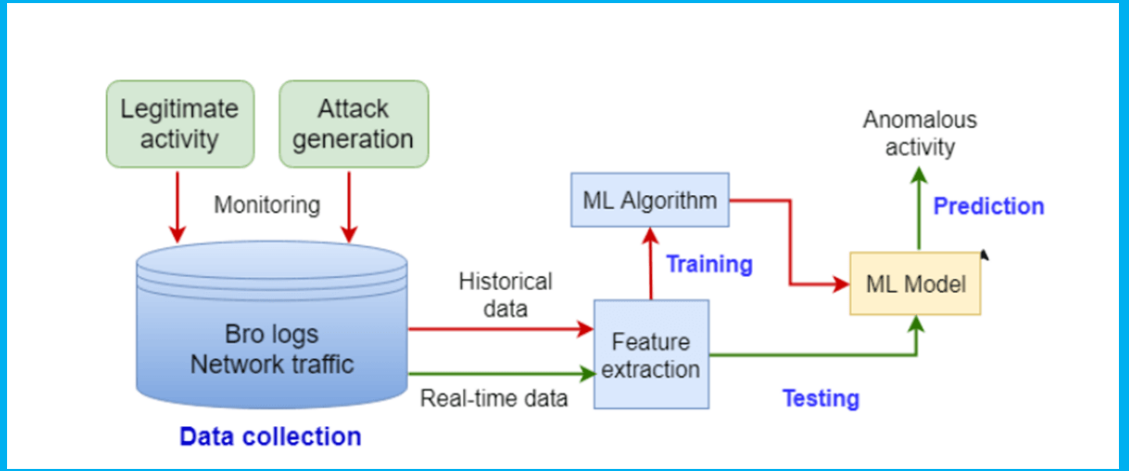
- **Signature detection**:

Signatures can be related to fingerprints. Many detection software use a database of known signatures of malwares and compare it with malware found in the system. But changing signature of a malware is very easy and can be done by just changing code and Hex values, so this method is not that effective.

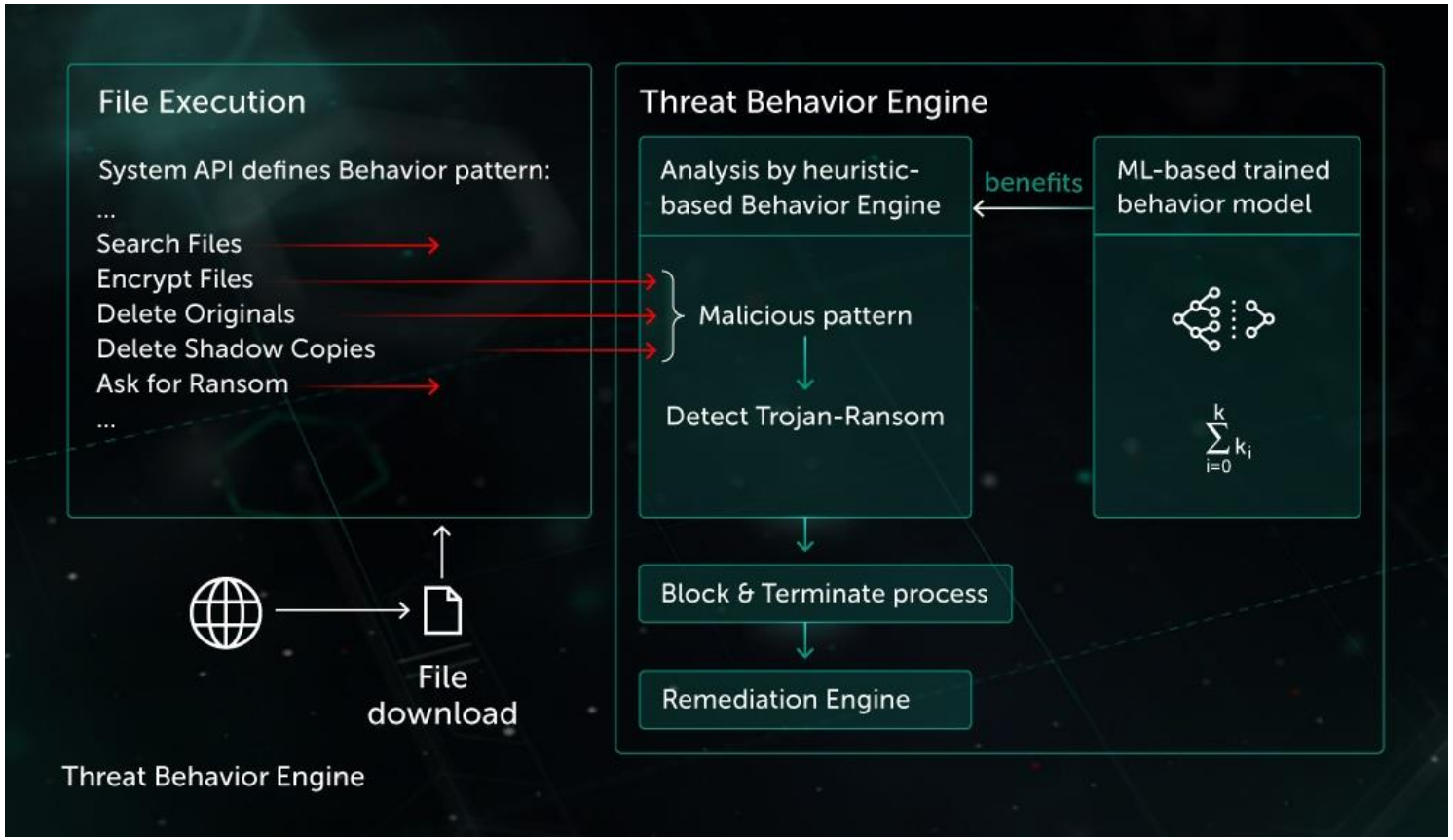


Abnormal traffic detection

- By using ML classification algorithms like logistic regression, random forests etc. , Reinforcement learning or Neural Networks using python language, many software are built which can classify that network traffic is suspicious or Ok and can take action accordingly.
- But one disadvantage is that traffic detection software generate many false-positives i.e. even if traffic is ok then also it marks it suspicious.



So now What?
Which method in ML can give us best possible results?



- Answer is design a ML program which can track **behavior** of files in our Operating System.
- It is just like that you are with a person since few weeks and now you know his/her behavior and can predict how would he/she react on particular situation.
- This is done by training ML model by using legal and trust worthy files in your system for few weeks so that it can predict when any external suspicious ransomware enters the system.