Ransomware

Definition, Danger & Prevention

- Malware ?
- Some Malware Type
- What is Ransomware ?
- Common Ransomware Attack Vectors
- Ransomware Lifecycle (Simple lab)
- Top Ransomware
- Prevention

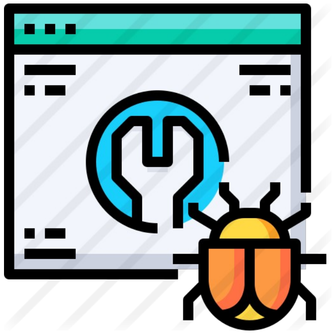
Malware ?

The term malware is a contraction of malicious software.

To make it simple,Malware is any piece of software that is designed with the intent to damage, disrupt or gain unauthorised access to people device and inflict harm to data and/or people in multiple ways.

Some Malware Types

- Virus: destroy system and slow down the performance.
- Worms: make copies of itself over and over — depleting system resources, such as hard drive space or bandwidth, by overloading a shared network.
- Spyware: Collects information and sends it to the hacker.
- Trojans: creating Back-doors that give other malware variants easy access.
- Bots & Botnets: control victim computer and use it in spam and phishing messages,... etc
- Ransomware

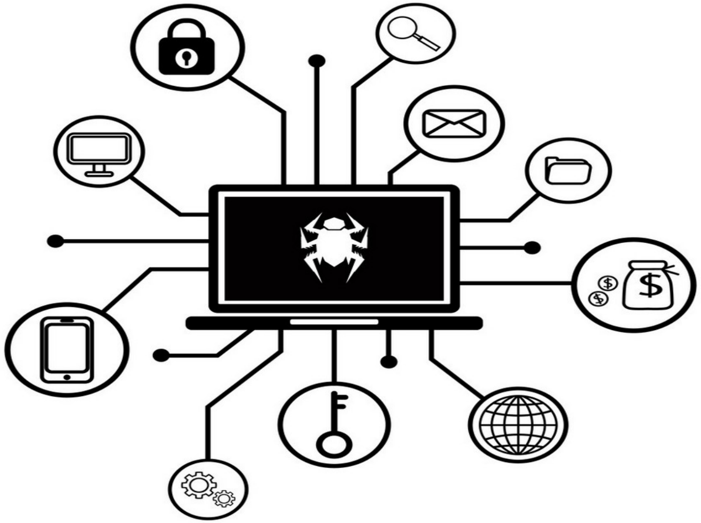


what is Ransomware

Ransomware is a type of malware that is designed to block user access from own system until a ransom fee is paid to ransomware creator.

Common Ransomware Attack Vectors

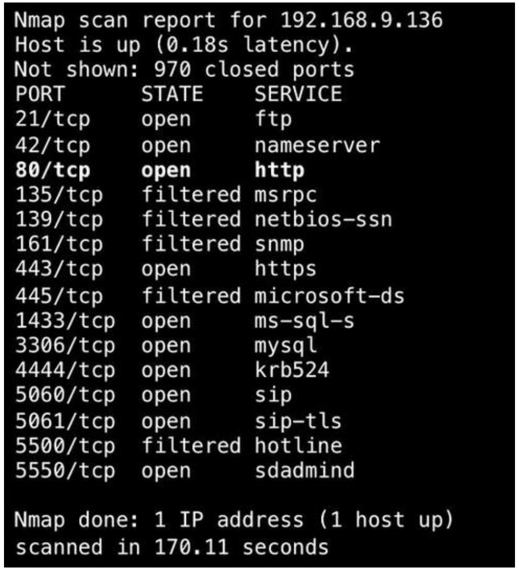
- Exploiting unsecured RDP ports (Remote Desktop Protocol)
- Brute forcing or dictionary attacks of weak passwords
- Sending phishing emails with malicious links or attachments
- Utilizing exploit kits to target known operating system vulnerabilities
- Gaining unauthorized access via out of date, unpatched software, servers, or firewalls



Unsecured RDP ports

- has been known since 2016 as a way to attack some computers and networks

- hackers have developed methods of identifying and exploiting vulnerable RDP sessions via the Internet to steal identities, login credentials and install and launch ransomware attacks.

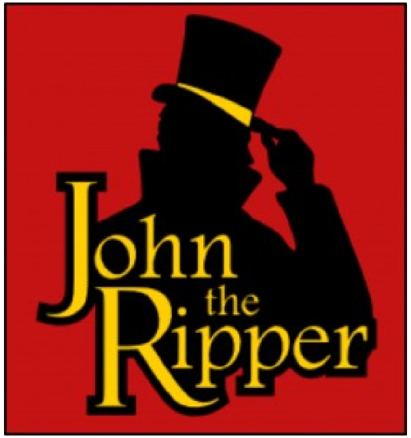


```
Nmap scan report for 192.168.9.136
Host is up (0.18s latency).
Not shown: 970 closed ports
PORT      STATE    SERVICE
21/tcp    open     ftp
42/tcp    open     nameserver
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
161/tcp   filtered snmp
443/tcp   open     https
445/tcp   filtered microsoft-ds
1433/tcp  open     ms-sql-s
3306/tcp  open     mysql
4444/tcp  open     krb524
5060/tcp  open     sip
5061/tcp  open     sip-tls
5500/tcp  filtered hotline
5550/tcp  open     sdadmind

Nmap done: 1 IP address (1 host up)
scanned in 170.11 seconds
```

Brute Forcing || Dictionary Attacks

- is a cryptographic hack that relies on guessing possible combinations of a targeted password until the correct password is discovered.



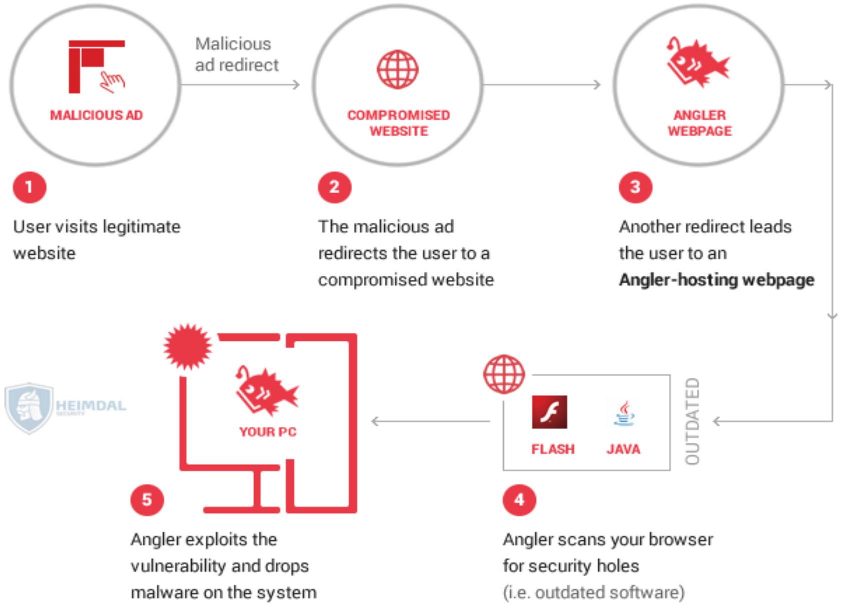
Phishing Attack

- type of social engineering attack use to trick users into doing 'the wrong thing', such as clicking a bad link that will download malware, or direct them to a dodgy(unsafe) website.

Bad Phishing Attack

exploit kits

- automatically and silently exploit vulnerabilities on victims' machines while browsing the web.



1 User visits legitimate website

2 The malicious ad redirects the user to a compromised website

3 Another redirect leads the user to an **Angler-hosting webpage**

4 Angler scans your browser for security holes (i.e. outdated software)

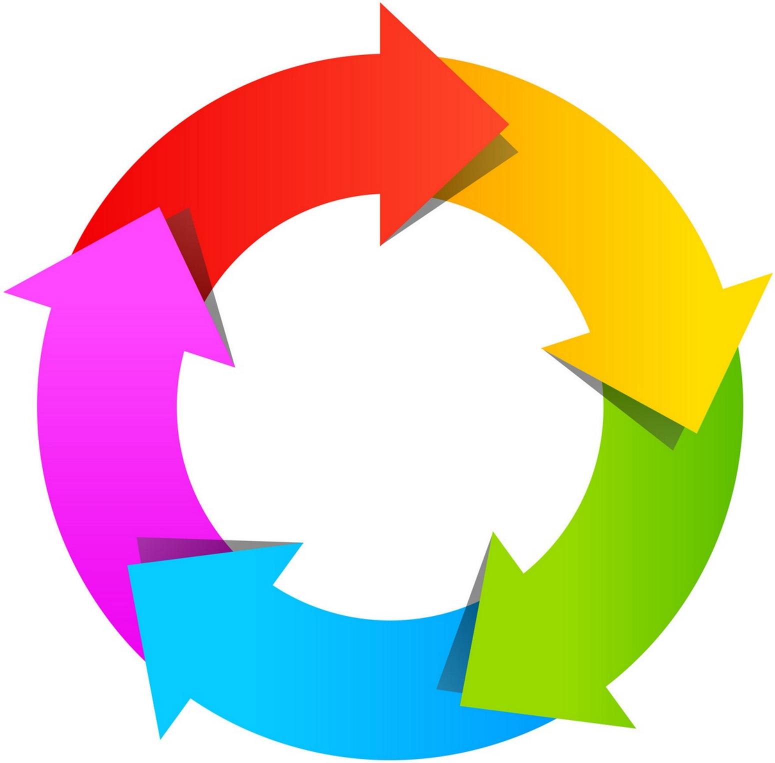
5 Angler exploits the vulnerability and drops malware on the system

Unauthorized access

- Out of date application ,serves , or even browser can lead to unauthorized access or install Malware into user device

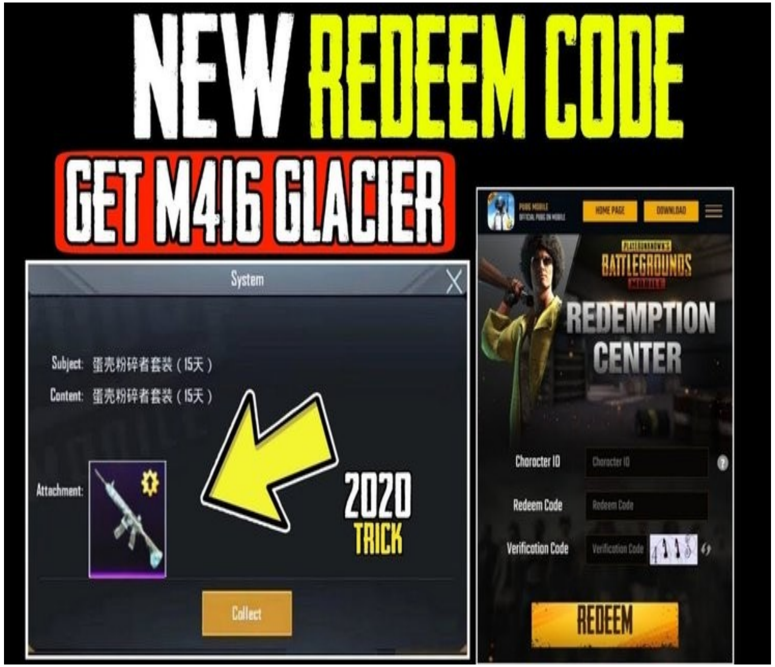
Ransomware Lifecycle

1) Distribution Campaign
2) Infection/Infiltration
3) Staging
4) Scanning (covert reconnaissance)
5) Encryption
6) Ransom Demand



Distribution Campaign

attackers use techniques like social engineering and weaponized websites to trick or force users to download a dropper which kicks off the infection



Subject: 蛋壳粉碎者套装（15天）

Content: 蛋壳粉碎者套装（15天）

Infection

file downloaded and code execution begins.

At this point your system has been infected with ransomware.

none of your files are encrypted yet.

It's important to note that at this point:

- all your automated detection controls have failed. all traffic are allowed .
- Malware check if it not in Sandbox Environment before start any action in this step

Staging

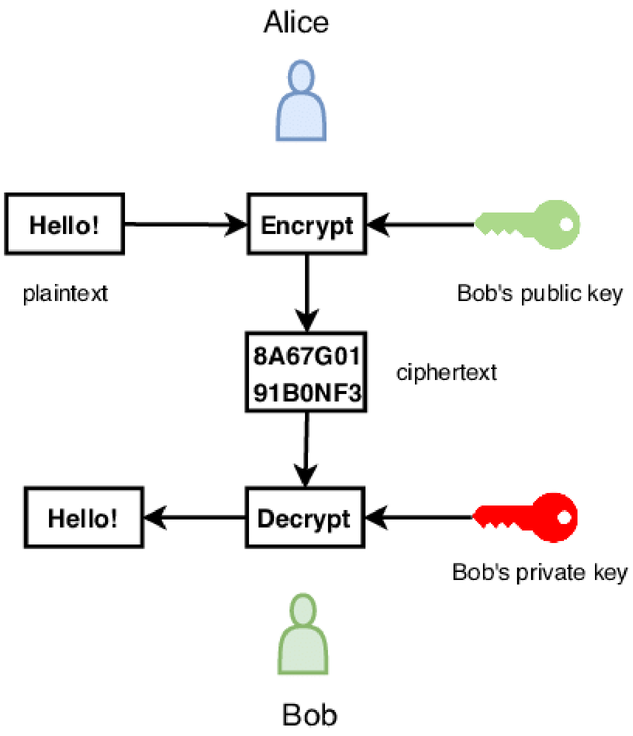
- the ransomware sets up, embeds itself in a system, and establishes persistency to exist beyond a reboot
- The attacker now “owns” the system.

Scanning (covert reconnaissance)

- Look, learn, and remain on the network. Get an understanding of how the network works, its vulnerabilities, and where the sensitive data is that will be worth a ransom
- ransomware searches for content to encrypt, both on the local computer and the network acces-sible resources

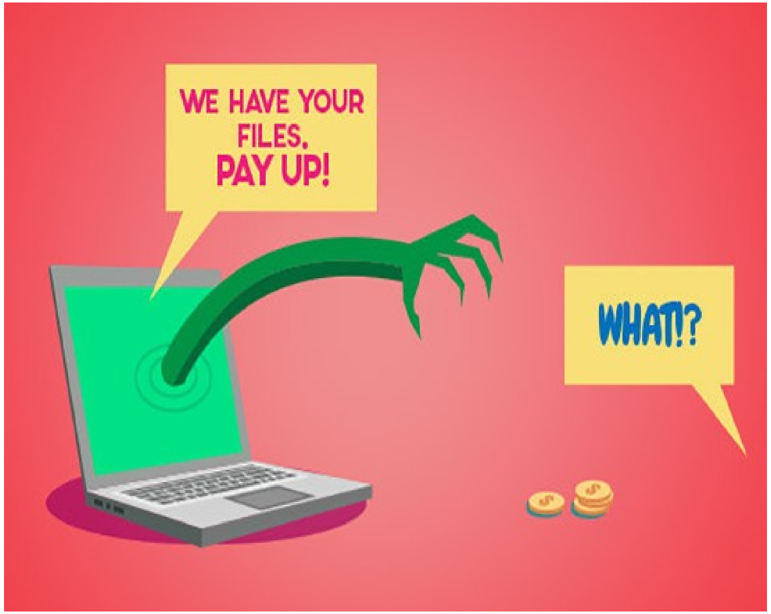
Encryption

- The discovered files are encrypted
- data on network file shares are copied down and encrypted locally, Then the encrypted files must be uploaded and the original files deleted.
-



Ransom Demand

A ransom note is generated, shown to the victim, and the hacker waits to collect on the ransom



Top Ransomware attack **2020**

- ISS World
  - Estimated cost: $74 million
  - recovery costs: between $22.5 million and $45 million
- Cognizant
  - Estimated cost: $50 million
  - recovery costs: $70 million
- Sopra Steria
  - Estimated cost: $50 million
  - recovery costs: $40 million and $50 million.

YOUR FILES ARE ENCRYPTED

Your photos, documents and other important files have been encrypted with unique key, generated for this computer.

Prevention

- Keep current data backups
- Scan emails for malware
- Not download files from unsafe site
- Check firewalls and endpoint protections
- Keep your OS, applications & serves up-to-date