COMPUTER ATTACKS

Information & Network Security

Mahati : 119
Samriddhi : 118
Nakul : 117
Keyur : 103

BRAIN VIRUS

INTERNET WORM

WEB BUG

TARGETED MALICIOUS CODE TRAP-DOORS

SALAMI ATTACK

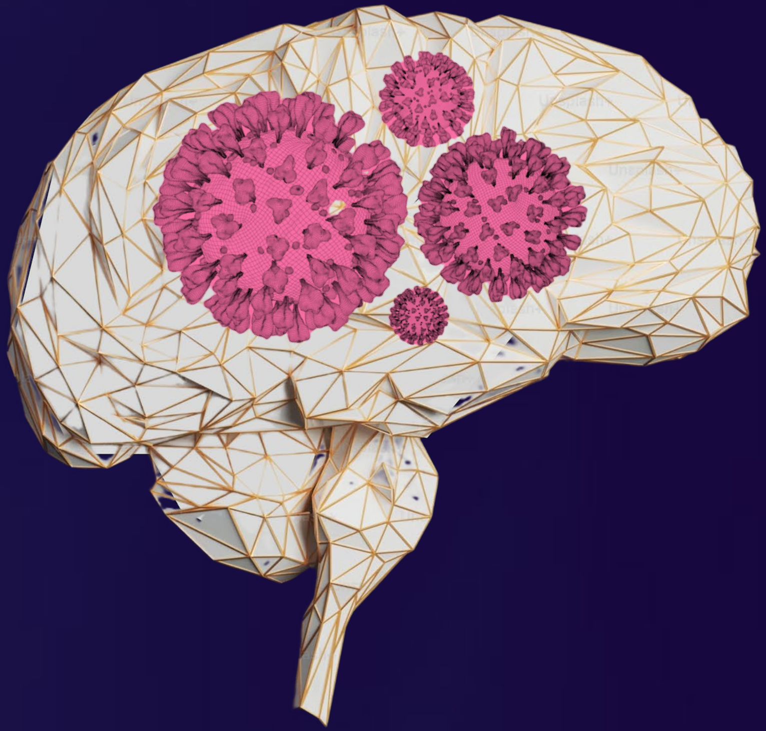
BRAIN VIRUS

The first computer virus, Brain, was discovered in 1986 and was created by two brothers, Basit and Amjad Farooq Alvi, who ran a computer store in Lahore, Pakistan.

The primary purpose of the virus was not to cause harm, but rather to protect the brothers' medical software from being copied without their permission.

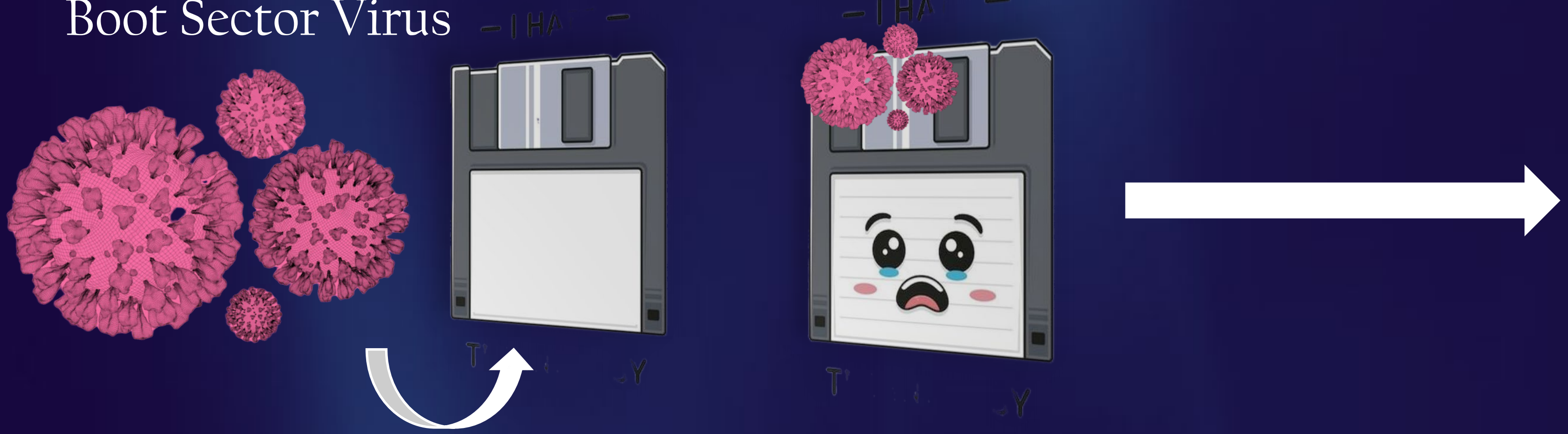
BRAIN VIRUS

- **Type**: Boot sector virus.
- **Target**: IBM PC-compatible computers running MS-DOS.
- **Infection Method**: The virus infects the boot sector of a floppy disk. When an infected disk is inserted into a computer, the virus loads into the computer's memory and infects the boot sector of any other floppy disks inserted afterward.



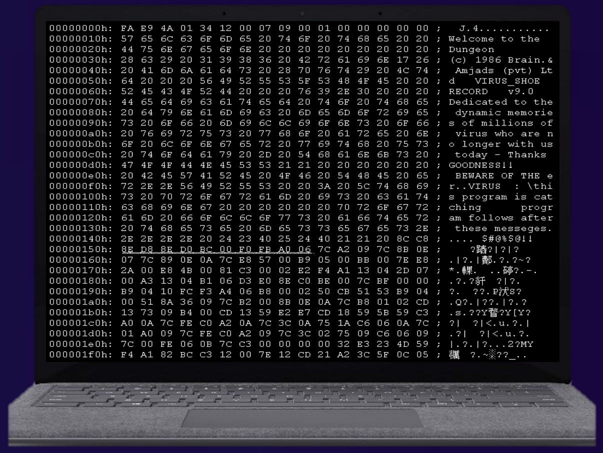
The boot sector is the area of a disk that is read by a computer's BIOS (Basic Input/Output System) when the computer is first starts up.

Boot Sector Virus



which means it infects the boot sector of floppy disks.

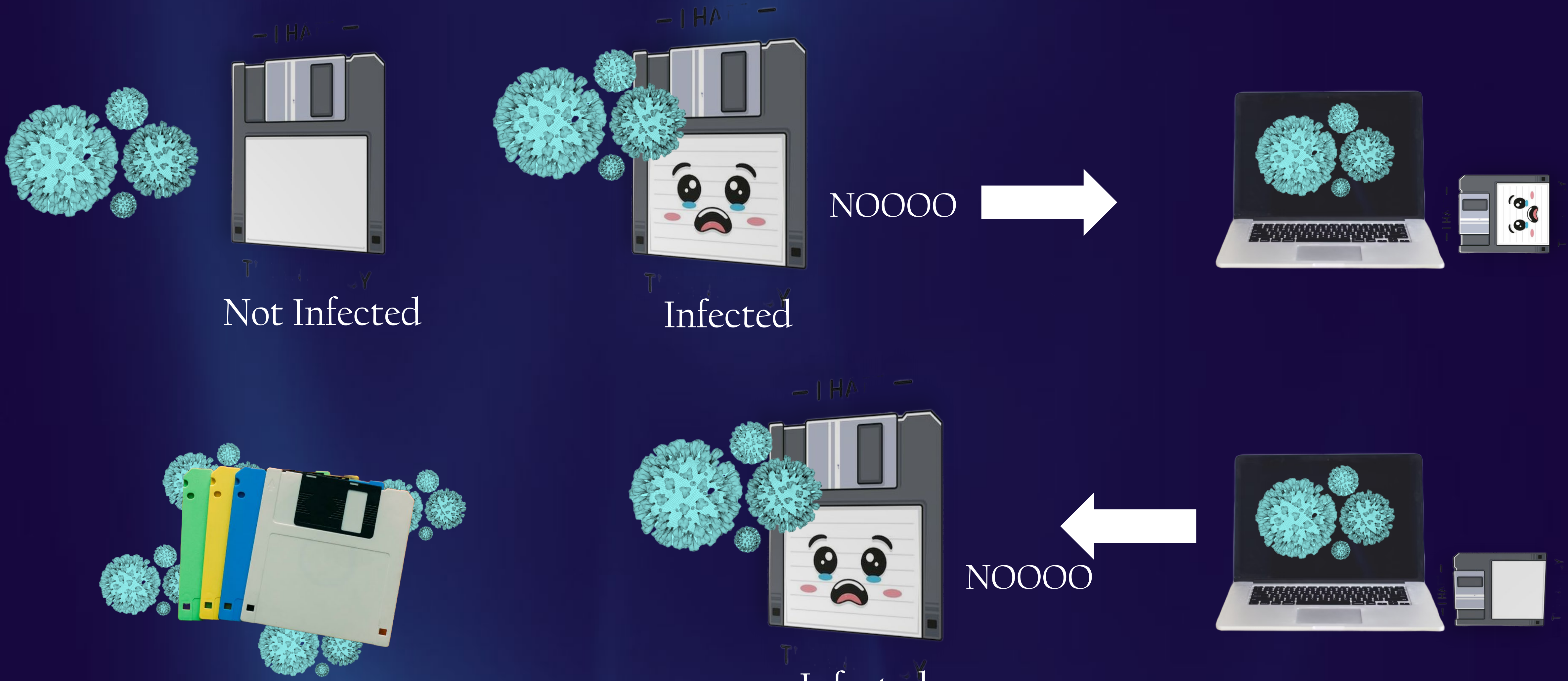
Infected System



```
00000000h: FA E9 4A 01 34 12 00 07 09 00 01 00 00 00 00 00 ;  J.4...........
00000010h: 57 65 6C 63 6F 6D 65 20 74 6F 20 74 68 65 20 20 ; Welcome to the
00000020h: 44 75 6E 67 65 6F 6E 20 20 20 20 20 20 20 20 20 ; Dungeon
00000030h: 28 63 29 20 31 39 38 36 20 42 72 61 69 6E 17 26 ; (c) 1986 Brain.&
00000040h: 20 41 6D 6A 61 64 73 20 28 70 76 74 29 20 4C 74 ;  Amjads (pvt) Lt
00000050h: 64 20 20 20 56 49 52 55 53 5F 53 48 4F 45 20 20 ; d   VIRUS_SHOE
00000060h: 52 45 43 4F 52 44 20 20 20 76 39 2E 30 20 20 20 ; RECORD   v9.0
00000070h: 44 65 64 69 63 61 74 65 64 20 74 6F 20 74 68 65 ; Dedicated to the
00000080h: 20 64 79 6E 61 6D 69 63 20 6D 65 6D 6F 72 69 65 ;  dynamic memorie
00000090h: 73 20 6F 66 20 6D 69 6C 6C 69 6F 6E 73 20 6F 66 ; s of millions of
000000a0h: 20 76 69 72 75 73 20 77 68 6F 20 61 72 65 20 6E ;  virus who are n
000000b0h: 6F 20 6C 6F 6E 67 65 72 20 77 69 74 68 20 75 73 ; o longer with us
000000c0h: 20 74 6F 64 61 79 20 2D 20 54 68 61 6E 6B 73 20 ;  today - Thanks
000000d0h: 47 4F 4F 44 4E 45 53 53 21 21 20 20 20 20 20 20 ; GOODNESS!!
000000e0h: 20 42 45 57 41 52 45 20 4F 46 20 54 48 45 20 65 ;  BEWARE OF THE e
000000f0h: 72 2E 2E 56 49 52 55 53 20 20 3A 20 5C 74 68 69 ; r..VIRUS  : \thi
00000100h: 73 20 70 72 6F 67 72 61 6D 20 69 73 20 63 61 74 ; s program is cat
00000110h: 63 68 69 6E 67 20 20 20 20 20 20 70 72 6F 67 72 ; ching      progr
00000120h: 61 6D 20 66 6F 6C 6C 6F 77 73 20 61 66 74 65 72 ; am follows after
00000130h: 20 74 68 65 73 65 20 6D 65 73 73 65 67 65 73 2E ;  these messeges.
00000140h: 2E 2E 2E 2E 20 24 23 40 25 24 40 21 21 20 8C C8 ; .... $#@%$@!!
00000150h: 8E D8 8E D0 BC 00 F0 FB A0 06 7C A2 09 7C 8B 0E ;    ?躇?|?|?
00000160h: 07 7C 89 0E 0A 7C E8 57 00 B9 05 00 BB 00 7E E8 ; .|?.|鄚.?.?~?
00000170h: 2A 00 E8 4B 00 81 C3 00 02 E2 F4 A1 13 04 2D 07 ; *.鑅.  ..磚?.-.
00000180h: 00 A3 13 04 B1 06 D3 E0 8E C0 BE 00 7C BF 00 00 ; .?.?鈃  ?|?.
00000190h: B9 04 10 FC F3 A4 06 B8 00 02 50 CB 51 53 B9 04 ; ?.  ??.P状S?
000001a0h: 00 51 8A 36 09 7C B2 00 8B 0E 0A 7C B8 01 02 CD ; .Q?.|??.|?.?
000001b0h: 13 73 09 B4 00 CD 13 59 E2 E7 CD 18 59 5B 59 C3 ; .s.??Y瞀?Y[Y?
000001c0h: A0 0A 7C FE C0 A2 0A 7C 3C 0A 75 1A C6 06 0A 7C ; ?|  ?|<.u.?.|
000001d0h: 01 A0 09 7C FE C0 A2 09 7C 3C 02 75 09 C6 06 09 ; .?|  ?|<.u.?.
000001e0h: 7C 00 FE 06 0B 7C C3 00 00 00 00 32 E3 23 4D 59 ; |.?.|?...2?MY
000001f0h: F4 A1 82 BC C3 12 00 7E 12 CD 21 A2 3C 5F 0C 05 ; 魌  ?.~░??_..
```

The virus was spread when users unknowingly infected their own systems by booting from an infected floppy disk.

SELF-REPLICATING VIRUS



Not Infected

Infected

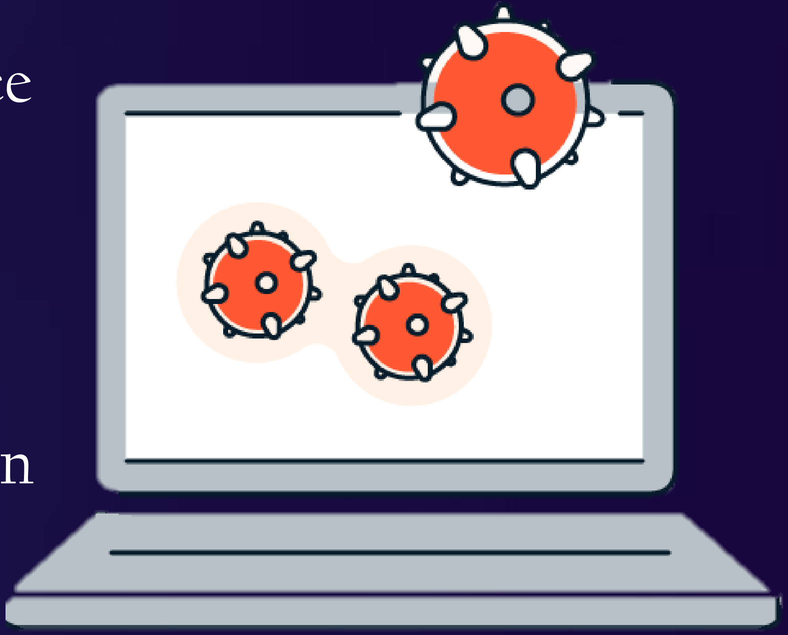
NOOOO

Infected

NOOOO

SELF-REPLICATING VIRUS

The virus replaces the original boot sector of a floppy disk with its own code, which is designed to check for the presence of the virus on the system it was infecting.



If the virus was not present, it would copy itself to the boot sector and then infect any other floppy disks that were used on the infected computer.

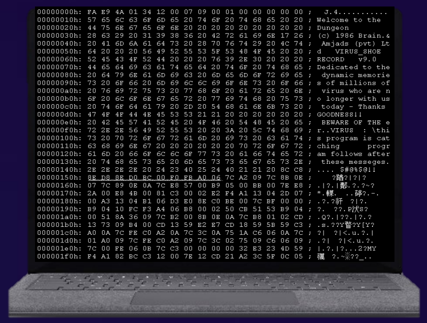
The virus was able to replicate itself and spread to other floppy disks, making it one of the first examples of a self-replicating virus

INFECTION

When a computer boots from an infected floppy disk, the virus loads into memory before the operating system. It then hooks into the system's disk I/O operations to ensure it remains active and continues to spread.

REPLICATION

The virus infects the boot sector of other floppy disks inserted into the computer. When these infected disks are used to boot other computers, the virus spreads further.

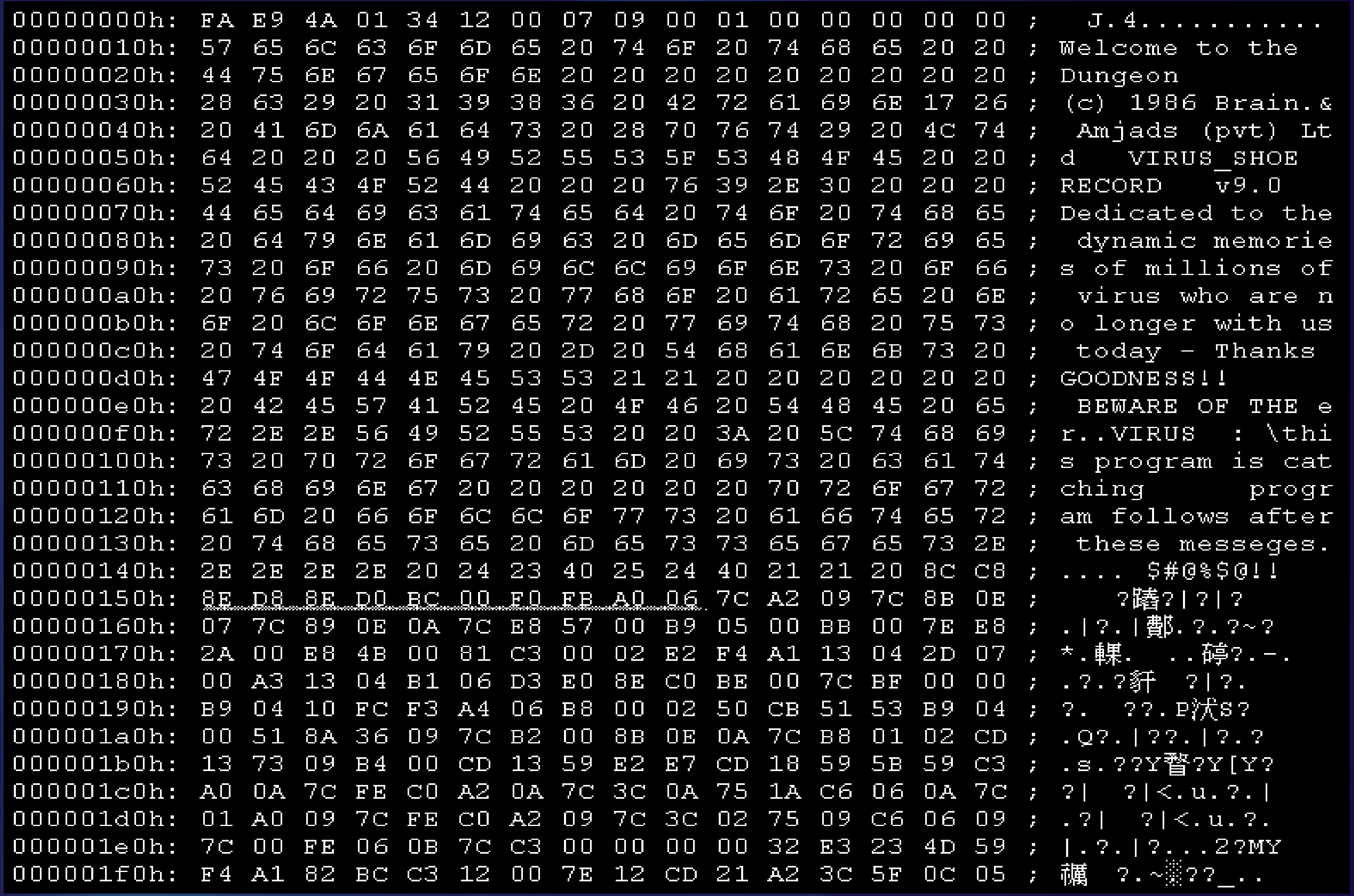


```
00000000h: FA E9 4A 01 34 12 00 07 09 00 01 00 00 00 00 00 ;  J.4...........
00000010h: 57 65 6C 63 6F 6D 65 20 74 6F 20 74 68 65 20 20 ; Welcome to the
00000020h: 44 75 6E 67 65 6F 6E 20 20 20 20 20 20 20 20 20 ; Dungeon
00000030h: 28 63 29 20 31 39 38 36 20 42 72 61 69 6E 17 26 ; (c) 1986 Brain.&
00000040h: 20 41 6D 6A 61 64 73 20 28 70 76 74 29 20 4C 74 ;  Amjads (pvt) Lt
00000050h: 64 20 20 20 56 49 52 55 53 5F 53 48 4F 45 20 20 ; d   VIRUS_SHOE
00000060h: 52 45 43 4F 52 44 20 20 20 76 39 2E 30 20 20 20 ; RECORD   v9.0
00000070h: 44 65 64 69 63 61 74 65 64 20 74 6F 20 74 68 65 ; Dedicated to the
00000080h: 20 64 79 6E 61 6D 69 63 20 6D 65 6D 6F 72 69 65 ;  dynamic memorie
00000090h: 73 20 6F 66 20 6D 69 6C 6C 69 6F 6E 73 20 6F 66 ; s of millions of
000000a0h: 20 76 69 72 75 73 20 77 68 6F 20 61 72 65 20 6E ;  virus who are n
000000b0h: 6F 20 6C 6F 6E 67 65 72 20 77 69 74 68 20 75 73 ; o longer with us
000000c0h: 20 74 6F 64 61 79 20 2D 20 54 68 61 6E 6B 73 20 ;  today - Thanks
000000d0h: 47 4F 4F 44 4E 45 53 53 21 21 20 20 20 20 20 20 ; GOODNESS!!
000000e0h: 20 42 45 57 41 52 45 20 4F 46 20 54 48 45 20 65 ;  BEWARE OF THE e
000000f0h: 72 2E 2E 56 49 52 55 53 20 20 3A 20 5C 74 68 69 ; r..VIRUS  : \thi
00000100h: 73 20 70 72 6F 67 72 61 6D 20 69 73 20 63 61 74 ; s program is cat
00000110h: 63 68 69 6E 67 20 20 20 20 20 20 70 72 6F 67 72 ; ching      progr
00000120h: 61 6D 20 66 6F 6C 6C 6F 77 73 20 61 66 74 65 72 ; am follows after
00000130h: 20 74 68 65 73 65 20 6D 65 73 73 65 67 65 73 2E ;  these messeges.
00000140h: 2E 2E 2E 2E 20 24 23 40 25 24 40 21 21 20 8C C8 ; .... $#@%$@!!
00000150h: 8E D8 8E D0 BC 00 F0 FB A0 06 7C A2 09 7C 8B 0E ;    ?踏?|?|?
00000160h: 07 7C 89 0E 0A 7C E8 57 00 B9 05 00 BB 00 7E E8 ; .|?.|鄚.?.?~?
00000170h: 2A 00 E8 4B 00 81 C3 00 02 E2 F4 A1 13 04 2D 07 ; *.鐉.  ..碠?.-.
00000180h: 00 A3 13 04 B1 06 D3 E0 8E C0 BE 00 7C BF 00 00 ; .?.?釬  ?|?.
00000190h: B9 04 10 FC F3 A4 06 B8 00 02 50 CB 51 53 B9 04 ; ?.  ??.P狀S?
000001a0h: 00 51 8A 36 09 7C B2 00 8B 0E 0A 7C B8 01 02 CD ; .Q?.|??.|?.?
000001b0h: 13 73 09 B4 00 CD 13 59 E2 E7 CD 18 59 5B 59 C3 ; .s.??Y晉?Y[Y?
000001c0h: A0 0A 7C FE C0 A2 0A 7C 3C 0A 75 1A C6 06 0A 7C ; ?|  ?|<.u.?.|
000001d0h: 01 A0 09 7C FE C0 A2 09 7C 3C 02 75 09 C6 06 09 ; .?|  ?|<.u.?.
000001e0h: 7C 00 FE 06 0B 7C C3 00 00 00 00 32 E3 23 4D 59 ; |.?.|?...2?MY
000001f0h: F4 A1 82 BC C3 12 00 7E 12 CD 21 A2 3C 5F 0C 05 ; 魽  ?.~▒??_..
```

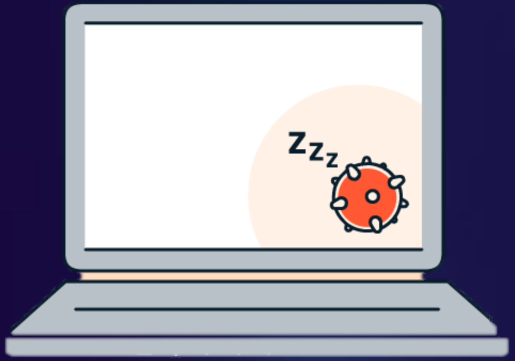
PAYLOAD

The Brain virus did not contain a destructive payload. Instead, it displayed a message indicating that the computer was infected, providing contact information for the creators in Pakistan.

WELCOME TO THE DUNGEON



```
00000000h: FA E9 4A 01 34 12 00 07 09 00 01 00 00 00 00 00 ;   J.4...........
00000010h: 57 65 6C 63 6F 6D 65 20 74 6F 20 74 68 65 20 20 ; Welcome to the  
00000020h: 44 75 6E 67 65 6F 6E 20 20 20 20 20 20 20 20 20 ; Dungeon         
00000030h: 28 63 29 20 31 39 38 36 20 42 72 61 69 6E 17 26 ; (c) 1986 Brain.&
00000040h: 20 41 6D 6A 61 64 73 20 28 70 76 74 29 20 4C 74 ;  Amjads (pvt) Lt
00000050h: 64 20 20 20 56 49 52 55 53 5F 53 48 4F 45 20 20 ; d   VIRUS_SHOE  
00000060h: 52 45 43 4F 52 44 20 20 20 76 39 2E 30 20 20 20 ; RECORD   v9.0   
00000070h: 44 65 64 69 63 61 74 65 64 20 74 6F 20 74 68 65 ; Dedicated to the
00000080h: 20 64 79 6E 61 6D 69 63 20 6D 65 6D 6F 72 69 65 ;  dynamic memorie
00000090h: 73 20 6F 66 20 6D 69 6C 6C 69 6F 6E 73 20 6F 66 ; s of millions of
000000a0h: 20 76 69 72 75 73 20 77 68 6F 20 61 72 65 20 6E ;  virus who are n
000000b0h: 6F 20 6C 6F 6E 67 65 72 20 77 69 74 68 20 75 73 ; o longer with us
000000c0h: 20 74 6F 64 61 79 20 2D 20 54 68 61 6E 6B 73 20 ;  today - Thanks 
000000d0h: 47 4F 4F 44 4E 45 53 53 21 21 20 20 20 20 20 20 ; GOODNESS!!      
000000e0h: 20 42 45 57 41 52 45 20 4F 46 20 54 48 45 20 65 ;  BEWARE OF THE e
000000f0h: 72 2E 2E 56 49 52 55 53 20 20 3A 20 5C 74 68 69 ; r..VIRUS  : \thi
00000100h: 73 20 70 72 6F 67 72 61 6D 20 69 73 20 63 61 74 ; s program is cat
00000110h: 63 68 69 6E 67 20 20 20 20 20 20 70 72 6F 67 72 ; ching      progr
00000120h: 61 6D 20 66 6F 6C 6C 6F 77 73 20 61 66 74 65 72 ; am follows after
00000130h: 20 74 68 65 73 65 20 6D 65 73 73 65 67 65 73 2E ;  these messeges.
00000140h: 2E 2E 2E 2E 20 24 23 40 25 24 40 21 21 20 8C C8 ; .... $#@%$@!!
00000150h: 8E D8 8E D0 BC 00 F0 FB A0 06 7C A2 09 7C 8B 0E ;     ?躇?|?|?
00000160h: 07 7C 89 0E 0A 7C E8 57 00 B9 05 00 BB 00 7E E8 ; .|?.|鄿.?.?~?
00000170h: 2A 00 E8 4B 00 81 C3 00 02 E2 F4 A1 13 04 2D 07 ; *.輮.  ..錞?.-.
00000180h: 00 A3 13 04 B1 06 D3 E0 8E C0 BE 00 7C BF 00 00 ; .?.?鉼  ?|?.
00000190h: B9 04 10 FC F3 A4 06 B8 00 02 50 CB 51 53 B9 04 ; ?.  ??.P狀S?
000001a0h: 00 51 8A 36 09 7C B2 00 8B 0E 0A 7C B8 01 02 CD ; .Q?.|??.|?.?
000001b0h: 13 73 09 B4 00 CD 13 59 E2 E7 CD 18 59 5B 59 C3 ; .s.??Y晵?Y[Y?
000001c0h: A0 0A 7C FE C0 A2 0A 7C 3C 0A 75 1A C6 06 0A 7C ; ?|  ?|<.u.?.|
000001d0h: 01 A0 09 7C FE C0 A2 09 7C 3C 02 75 09 C6 06 09 ; .?|  ?|<.u.?.
000001e0h: 7C 00 FE 06 0B 7C C3 00 00 00 00 32 E3 23 4D 59 ; |.?.|?...2?MY
000001f0h: F4 A1 82 BC C3 12 00 7E 12 CD 21 A2 3C 5F 0C 05 ; 襶  ?.~░??_..
```



NON-DESCRUCTIVE

Unlike many later viruses, the Brain virus did not cause harm to data or system functionality. Its main effect was to propagate itself and display the embedded message.

AWARENESS

The Brain virus played a significant role in raising awareness about computer security and the potential for malicious software to spread.

LEGACY

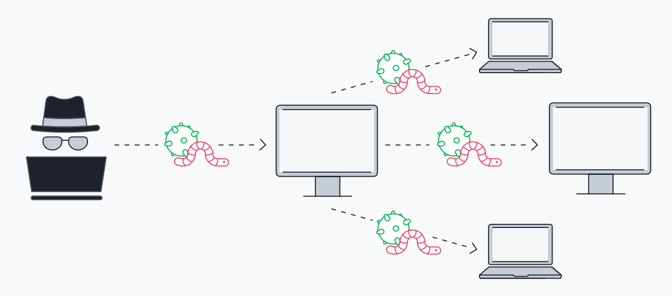
As one of the first widely known computer viruses, the Brain virus has a significant place in the history of computer security. It highlighted the vulnerabilities in early computer systems and the need for protective measures such as antivirus software.

INTERNET WORM

An Internet worm is type of malicious software (malware) that self-replicates and distributes copies of itself to its network. These independent virtual viruses spread through the Internet, break into computers, and replicate without intervention from and unbeknownst to computer users.

Key Characteristics:

1) Self-Replication :



2) Exploitation of vulnerabilities : They often exploit security flaws in software or network services to gain access to systems.

3) Network impact : Worms can cause significant disruptions by consuming bandwidth, overloading servers, and slowing down network performance.

4) Payloads : Some worms carry additional malicious payloads, such as spyware, ransomware, or backdoors, which can further compromise affected systems.

HOW DO WE KNOW THAT THE WORM IS IN OUR SYSTEM !

PREVENTION AND MITIGATION

1) Regular Software Update :

- Patch Management:
- Operating System Updates:
- Application Updates:

2) Firewalls And Intrusion Detection Systems :

- Network Firewalls:
- Host-based Firewalls:
- Intrusion Detection and Prevention Systems (IDPS):

PREVENTION AND MITIGATION

3) Antivirus and Antimalware Programs :

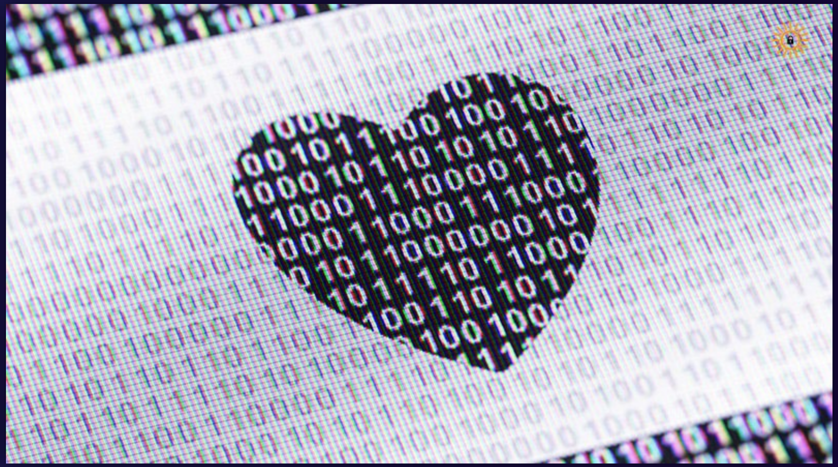
- Real-time Protection:
- Regular Scans:
- Signature and Heuristic Analysis:

4) Backup and Recovery

- Regular Backups:
- Backup Verification:

NOTABLE EXAMPLES :

- Morris Worm (1988):
- ILOVEYOU Worm (2000):
- WannaCry (2017):



WEB BUGS

A Web bug is a hidden, transparent, but nonetheless "graphic" image that finds its way onto your computer. They're small "objects" that are embedded into a webpage or an email and are "activated" when you visit the site or open the email.

Web bugs, also known as "tags," "tracking bugs," "pixel trackers," or "pixel GIFs," are tiny, invisible images typically no larger than 1x1 pixel. They appear in a graphical format called GIF (Graphic Interchange Format), common on the Web. To your browser, they look just like any other image, making them blend in seamlessly. As a result, both users and browsers fail to recognize their presence. These web bugs are often used for tracking purposes.

How do Web bugs get on your computer?

A Web bug gets your computer through an email, or it can be in a webpage that you visit. Some people might call it "spyware," in that it's used to take note of your online activity, but in most cases (especially with websites) it's not there to do any harm.

What are Web bugs up to?

Web bugs track in specific, purposeful ways some of your online behaviour when you receive an email or visit a specific website. Web bugs are custom-made: They are designed to monitor your activity (individually or as part of all website visitors) to give somebody helpful information.

Website owners use Web bugs to know how many people visited their website. And ad networks (advertising companies focusing on the Web) use them to get customer behavior data. They'll use Web bugs in their ads to get an idea of how often an advertisement is appearing or being viewed. They can also use Web bugs to track an individual's response to online ads (one by one).

What are Web bugs up to?

- It can gather the IP address of the computer
- The URL of the web page the bug is located on
- The URL of the page the bug came from
- The time the bug was observed
- Set a cookie value

How to Prevent or Protect Yourself from Web Bugs

Use Browser Extensions	Email Security	Browser Privacy Settings
• Ad Blockers • Privacy Extensions	• Disable Image Loading • Secure Email Services	• Block Third-Party Cookies • Do Not Track

Network-Level Protection	Clear Cookies and Cache	Monitor Permissions
• Use VPN • Privacy DNS services	• Frequently clear cookies and browser cache to remove tracking data.	• Review Site Permissions • Disable JavaScript

TARGETED MALICIOUS CODE

Targeted malicious code is specialized malware developed to compromise a specific individual, organization, or system. It is crafted to exploit distinct vulnerabilities and achieve particular objectives, such as unauthorized access, data theft, or surveillance, rather than indiscriminately affecting a broad range of users.

Trapdoors

A trapdoor is an undocumented entry point to a module. The trapdoor is inserted during code development, perhaps to test the module, to provide "hooks" by which to connect future modifications or enhancements or to allow access if the module should fail in the future. In addition to these legitimate uses, trapdoors can allow a programmer access to a program once it is placed in production.

- A trap door is a secret backdoor mechanism built into a system that allows an authorized person to access the system or specific functionality in a hidden way.
- It is often added to software or hardware systems by the system designer or developer, and is not disclosed to the end user or system administrator.
- The purpose of a trap door is to provide an emergency access mechanism that can be used by a system administrator to recover from a system failure or perform system maintenance activities.
- Trap doors can also be exploited by attackers to gain unauthorized access or control over a system.
- In some cases, a trap door may be intentionally added by an attacker during the development phase, enabling them to gain access to the system at a later time.

Causes of Trapdoors :

Developers usually remove trapdoors during program development, once their intended usefulness is spent. However, trapdoors can persist in production programs because the developers

forget to remove them

intentionally leave them in the program for *testing*

intentionally leave them in the program for *maintenance* of the finished program, or

intentionally leave them in the program as a *covert means of access* to the component after it becomes an accepted part of a production system

Trapdoors Examples

- 1980: In the 1980s, the US National Security Agency (NSA) was accused of including a trap door in the Unix operating system that was distributed to foreign governments. The trap door was reportedly designed to allow the US government to gain access to the systems of foreign governments that were using the Unix operating system.

- 2004: In 2004, a researcher discovered a trap door in the Diebold Election Systems voting machines used in the US. The trap door was designed to allow election officials to update the software on the machines, but it was not disclosed to the public or election officials, making it a potential target for attackers.

- 2013: In 2013, it was reported that the NSA had a program called Bullrun, which involved inserting trap doors into commercial encryption products, such as virtual private network (VPN) software, to enable the NSA to bypass the encryption and gain access to the encrypted data

Preventing Trapdoors

Trapdoors, or backdoors, are secret ways to access a system without authorization. Here are key steps to prevent them:

1. Secure Development
    - ❖ Review Code: Regularly check code for hidden backdoors.
    - ❖ Use Analysis Tools: Scan code for vulnerabilities.

2. Access Controls
    - ❖ Limit Access: Give users only the access they need.
    - ❖ Multi-Factor Authentication: Use MFA for critical systems.
    - ❖ Audit Logs: Track and review access to sensitive code.

Preventing Trapdoors

3. System Audits

- Scan for Vulnerabilities: Regularly scan systems for weaknesses.
- Penetration Testing: Simulate attacks to find backdoors.

4. Network and System Security

- Disable Unneeded Services: Turn off unnecessary features.
- Use Firewalls and IDS: Monitor and control network traffic.

5. Monitoring

- Continuous Monitoring: Watch for unusual system activity.
- File Integrity Checks: Detect unauthorized file changes.

The Salami Attack

- A salami attack is a method of cybercrime that attackers or a hacker typically used to commit financial crimes.

- Cybercriminals steal money or resources from financial accounts on a system one at a time.

- This attack occurs when several minor attacks combine to create a sturdy attack. because of this sort of cybercrime, these attacks frequently go undetected.

- A salami attack is the theft of small amounts of money from a large number of accounts, often over a long period of time. It is named after the method of slicing thin slices of salami, as the thief is able to steal small amounts of money from many accounts without being noticed

Working of Salami Attack

- During this kind of attack, an awfully insignificant change is introduced that goes completely unnoticed.

- As an example, the attacker inserts a program, into the bank's servers, that deducts a satiny low amount of cash from the account of each customer.

- No account holder will probably notice this unauthorized debit, but the attacker will make an outsized amount of cash each month.

Types of Salami Attack

Salami Slicing:

- Salami Slicing occurs when the attacker gets customer information, like debit/credit card details and other similar sort of detail by using an online database.

- The attacker then deduct an awful touch of cash from each account and these amounts add up to an oversized amount of cash and this can be often invisible to detect such amount, since the amount is tiny

Penny Shaving:

- A penny-shaving attack is similar to a salami-slicing attack, but it involves the manipulation of financial transactions in order to steal small amounts of money from a single account over a long period of time.

- The attacker infiltrates a company's financial system and begins making small, unauthorized changes to the amounts of financial transactions, such as rounding down the amount by a few cents or dollars and stealing a large amount of money from several bank accounts

Preventions from Salami Attack

- Users are encouraged to oversee their weekly transactions and month-to-month bank statements to shield their bank accounts from being hindered by a salami attack.

- You'll monitor any potential charges on your account by actively scanning through these activities.

- If you have got any issues with any strange charges on your account, contact your bank.

- Financial institutions, like banks, should also update their security so that the attacker doesn't become conversant in how the framework is meant.

- Banks should advise customers on the due to report any money deduction that they weren't tuned in to.

THANK YOU !