কমপিউটার ভাইরাস ঃ পরিচিতি, প্রভাব ও প্রতিকার

নির্মল চন্দ্র চৌধুরী

(পূর্ব প্রকাশিতের পর)

৭। **ইয়্যাল ভাইরাস** (Yale Virus) :

• অপর নাম – অ্যালামেদা ভাইরাস।

• শুধুমাত্র ৩৬০ কেবি বিশিষ্ট ফ্লপি ডিস্ক আক্রমণ করে।

• আক্রান্ত ডিস্কের মূল বুট সেক্টরকে ০ সাইডের ৮ নং সেক্টরের ৩৯ নং ট্র্যাকে স্থানান্তরিত করে। এবং আক্রমণের পূর্বে ঐ স্থানে কোন তথ্য থেকে থাকলে তা নষ্ট করে ফেলে।

• মেমোরীতে ভাইরাস অবস্থানকালে কোন অনাক্রান্ত ডিস্ক ড্রাইভে ঢুকিয়ে Alt+Ctrl+Del কী সমন্বয়ে কমপিউটার পুণঃচালিত করলে ভাইরাসটি ঐ ডিস্কটিকে আক্রমণ করে।

৮। **দেন-জুক ভাইরাস** (Den-Zuk Virus) :

• শুধুমাত্র ৩৬০ কেবি বিশিষ্ট ফ্লপি ডিস্ক আক্রমণ করে।

• স্বয়ংক্রিয়ভাবে মেমোরীতে লোড হয় এবং BIOS-এর হিসেবে মেমোরীর অবশিষ্ট পরিমাণ (Available Memory) ৭ কিলোবাইট কমতি দেখায়।

• এটি ডিস্কটিকে একটি ভিন্ন আঙ্গিকে ফর্ম্যাট করে; যেখানে সাধারণ ১–৯ সেক্টরকে নামকরণ করে ৩৩–৪২ সংখ্যায় এবং মূল বুট সেক্টরকে ০ সাইডের ৪০ নং ট্র্যাকে স্থানান্তরিত করে।

• ভাইরাসটি ডিস্ক আই/ও (১৩) এবং কী বোর্ড (৯) ফাংশনকে বাঁধাগ্রস্থ করে।

• Alt+Ctrl+Del কী সমন্বয়ে কমপিউটার পুনঃচালিত করলে ভাইরাসটি স্ক্রীণে Den -Zuk Logo-এর একটা সুন্দর ছবি প্রদর্শন করে (কেবলমাত্র গ্রাফিক্স স্ক্রীনে)।

ভূমিকা ভিত্তিক শ্রেণীবিভাগ ঃ

এ শ্রেণীবিভাগটি করা হয়েছে আসলে পূর্বে আলোচিত ভাইরাসগুলোর ভূমিকার ধরণ অনুসারে। ফলে ভাইরাসগুলো নতুন করে আলোচনার অবকাশ নেই। বরং ভূমিকা অনুসারে নিম্নে এর একটা তালিকা দেয়া হল।

(ক) মেমোরী বিনষ্টকারী ভাইরাস ঃ

আসলে প্রতিটি ভাইরাসই তার কর্মকাণ্ডের প্রারম্ভে কমপিউটারের মেমোরীতে অবস্থান নেয়। এতে স্বভাবতঃ মেমোরীর কিছুটা জায়গার অপচয় ঘটে যা প্রতিটি ভাইরাসের আকারের সমান। তবে কিছু ভাইরাস রয়েছে পূর্বে আলোচিত হয়নি যেগুলোর তেমন কোন ক্ষতিকর ভূমিকা নেই। শুধু মোমোরীতে অবস্থান নিয়ে মেমোরীর কিছুটা জায়গা দখল করে এবং অন্যান্য ডিস্কে সংক্রমিত হয়। এদের মধ্যে রয়েছে —

১। **অ্যামস্ট্রাড কম ভাইরাস** (AMSTARD COM VIRUS) :

• আকার – ৮৫০ বাইট

• শুধুমাত্র COM ফাইল আক্রমণ করে, তবে COMMAND. COM ফাইল আক্রমণ করে না।

২। **৬৪০ কে কম ভাইরাস** (640 K Com Virus) ঃ

• আকার – ৫৮৩ বাইট

• শুধুমাত্র COM ফাইল আক্রমন করে।

• নিজেই নিজেকে মেমোরীর ৯৮০০ : ০০০০ অবস্থান কপি করে নিয়ে অবস্থান করে। এ জন্যে এটি কেবল ৬৪০ কেবি মেমোরীর কমপিউটারগুলোতেই প্রয়োগ হয়।

(খ) ডিস্ক বিনষ্টকারী ভাইরাস সমূহ ঃ

নিম্নের ভাইরাসগুলো এ পর্যায়ভূক্ত —

১। ১৪ই শনিবার ভাইরাস
২। রবিবার ভাইরাস
৩। ক্রীষ্টমাস ভাইরাস
৪। ড্যাটাক্রাইম ভাইরাস
৫। লিহাই ভাইরাস

(গ) ফাইল বিনষ্টকারী ভাইরাস সমূহ ঃ

১। ১৩ই শুক্রবার ভাইরাস
২। ১লা মঙ্গলবার ভাইরাস
৩। ওরোপ্যাক্স ভাইরাস
৪। অ্যালাবামা ভাইরাস
৫। শতবছর ভাইরাস
৬। ভিয়েনা ভাইরাস
৭। প্রিটোরিয়া ভাইরাস
৮। সিলভিয়া ভাইরাস
৯। ভূত ভাইরাস
১০। ১৭২০ ভাইরাস
১১। জিরো বাগ ভাইরাস
১২। এইডস ভাইরাস
১৩। তাইওয়ান ভাইরাস
১৪। ব্রেসলোনা ভাইরাস
১৫। ৫১২০ ভাইরাস

ট্রোজান (Trojans)

ট্রোজান হচ্ছে একধরনের ধোঁকা দেয়া প্রোগ্রাম। কোন ভাল কাজের উদ্দেশ্যে লেখা কোন প্রোগ্রামের মধ্যে প্রোগ্রামার সুকৌশলে এমন কিছু নির্দেশ রেখে দেয় যা ভাল প্রোগ্রামের ছদ্মাবরণে থেকে ভারাসের মত খারাপ কাজ করে। ব্যবহারকারী হয়তো ভাল কোন উদ্দেশ্য নিয়ে প্রোগ্রামটি প্রয়োগ করছেন কিন্তু আসলে তিনি নিজের অজান্তে নিজের ক্ষতি করে ফেলছেন। ঠিক যেন দধি ভেবে চুন খাওয়ার মত অবস্থা। অবশ্য এগুলো চিহ্নিত করা সাধারণ ব্যবহারকারীর জন্য একটু কষ্টকর।

কখনও কখনও প্রোগ্রামারের অদক্ষতা বা অসাবধানতার কারণেও প্রোগ্রামের মধ্যে তার অজান্তে এ জাতীয় খারাপ বা বিপরীত ভূমিকাকারী নির্দেশ যুক্ত হয়ে যায়।

ভাইরাসের প্রতিকার ঃ

ভাইরাসের আক্রমণ প্রতিহত করতে হলে প্রথমেই নিশ্চিত হওয়া প্রয়োজন আপনার মেশিন বা ডিস্কটি সত্যি সত্যিই ভাইরাস কর্তৃক আক্রান্ত হয়েছে কি-না ? হয়ে থাকলে কোন ধরণের কি ভাইরাস ? এ নিশ্চিত হওয়ারও কতগুলো পন্থা রয়েছে।

যে সমস্ত উপসর্গ থেকে ভাইরাসের উপস্থিতি অনুমান করা যায় বা নিশ্চিত হওয়া যায় তার মধ্যে রয়েছে —

সিপিইউ কেন্দ্রিক উপসর্গ ঃ

* **মেমোরী কম প্রদর্শন ঃ** সাধারণ ভাবে ডসের CHKDSK কম্যাণ্ড ববহার করে কমপিউটারের ইনস্টলড মেমোরীর পরিমাণ জানা যায়। একটি ৬৪০ কেবি র‍্যাম বিশিষ্ট কমপিউটারের মেমোরী হওয়ার কথা ৬৫৫৩৬০ বাইট (৬৪০×১০২৪)। ভাইরাস আক্রান্ত হলে এ পরিমাণ কম হবে। তবে এ কমের পরিমাণ সাধারণতঃ ৩ কেবি থেকে ৯ কেবি এর মধ্যে থাকে যা আক্রান্ত

ভাইরাসের আকারের ওপর নির্ভর করে। কোন কমপিউটারে বর্ধিত মেমোরী (Expanded Extended Memory) থাকলে সেক্ষেত্রে ডস ৪.০ এর কম ভার্শন গুলোর ৬৪০ কেবি দেখাতে পারে (যেক্ষেত্রে হয়ত মোট মেমোরী ১ এমবি এতে ৩৮৪ কেবি ভাইরাস কর্তৃক দখলকৃত বলে মনে হতে পারে। কিন্তু তা অসম্ভব। সুতরাং এরূপ ক্ষেত্রে অতিরিক্ত মেমোরীর পরিমাণ বিয়োগ করে হিসেব করতে হবে।

* **নিয়মিত প্রোগ্রাম ক্র্যাশ করা :** মেশিনে কোন প্রোগ্রাম চালাতে গেলে যদি প্রতিবারই একটা নির্দিষ্ট নিয়মে সিস্টেম ক্র্যাশড্ বা হ্যাঙড্ হয়ে যায় তাহলেও ভাইরাসের উপস্থিতি সন্দেহ করা যেতে পারে। তবে মেশিনের কোন হার্ডওয়্যার সমস্যার কারণেও এমনটি হতে পারে ; সেক্ষেত্রে হার্ডওয়্যার প্রকৌশলী দেখিয়ে নিশ্চিত হয়ে নিন।

* **ঠিকমত ইনপুট/আউটপুট না দেয়া :** কখনও ভাইরাসের আক্রমণে মেশিনের ইনপুট/আউটপুট ডিভাইসগুলো ঠিকমত কাজ করে না। যেমন ডিস্ক রিড/রাইট এরর, মনিটর হ্যাঙড্ হওয়া ইত্যাদি। মেশিনের সাথে টেলেক্স বা ফ্যাক্স কার্ড লাগানো থাকলে সেগুলোও ভাইরাসের উপস্থিতিতে হ্যাঙড্ হয়ে যায়।

* **ধীর তথ্য প্রক্রিয়াকরণ :** ভাইরাস অনেক সময় ইনপুট/আউটপুটের চলাচল (Flow) কে বাঁধাগ্রস্থ করে কমপিউটারের তথ্য প্রক্রিয়াকরণের গতি কমিয়ে দেয়।

ডিস্ক ভিত্তিক উপসর্গ :

ব্যাডসেক্টর : ভাইরাস কর্তৃক আক্রান্ত হলে একটা ডিস্কে ব্যাডসেক্টর উৎপন্ন হয়। বুট সেক্টর ভাইরাসগুলো ভাইরাস প্রোগ্রামের প্রথম অংশ বুট সেক্টরে সঞ্চিত করে এবং বাকী অংশ ড্যাটা অংশে সঞ্চিত করে। শেষোক্ত অংশটিকে ব্যাডসেক্টর হিসেবে চিহ্নিত করে যাতে ডস ঐ অংশটা ব্যবহার থেকে বিরত থাকে।

* **ডিস্ক অ্যাক্সেজ টাইম বৃদ্ধি পাওয়া :** অনেক সময় কমপিউটার কোন ডিস্ক থেকে ফাইল পড়তে বা ডিস্কে ফাইল লিখতে বেশ সময় নেয়। এটা ভাইরাসের উপস্থিতির কারণে হতে পারে। ভাইরাসটি যদি বুট সেক্টর আক্রমনের চেষ্টা করে তাহলে অ্যাকসেজ টাইম বেড়ে যায়।

* **ডিস্কে শুণ্যস্থানের কমতি হওয়া :** অনেক সময় দেখা যায় ডিস্কে সংগৃহীত ফাইলের সংখ্যা অনাকাংখিত ভাবে বেড়ে গেছে। স্বাভাবিকভাবেই এতে ডিস্কের ফাঁকা জায়গার পরিমাণ কমে যায়। এটি ঘটে ভাইরাস কর্তৃক তৈরীকৃত নতুন কোন ফাইল সৃষ্টি বা বর্তমান ফাইলের আকার বেড়ে যাওয়ার কারণে।

* **ড্রাইভ পড়ায় বিলম্ব ঘটা :** অনেক ক্ষেত্রে একটা ডিস্ক থেকে কোন তথ্য পড়ার সময় ড্রাইভ হুইল বেশী সময় ধরে ঘুড়তে থাকে। মেমোরীতে ভাইরাসের উপস্থিতি থাকলে এরূপ ঘটতে পারে। কেননা ভাইরাসটি ডিস্কে তার উপস্থিতি ও অবস্থান খুঁজে। এটা নিশ্চিৎ হওয়ার একটা সহজ পথ হচ্ছে একটা ভাল ডিস্ককে রাইট প্রটেক্টর ট্যাগ লাগিয়ে তার ডাইরেক্টরী লিষ্ট করার কম্যাণ্ড দেওয়া। এক্ষেত্রে ভাইরাসটি বুট সেক্টর ভাইরাস হলে লক্ষ্য ডিস্কের বুট সেক্টরে নিজেকে কপি করতে যাবে কিন্তু রাইট প্রটেক্টরের কারণে তা বিলম্বিত হবে অর্থাৎ ড্রাইভ লাইট অনেক ক্ষন ধরে জ্বলবে এবং এক পর্যায়ে যখন ব্যর্থ হবে তখন ডস একটা মেসেজ দিবে Write protect error in drive A, যা কিছু কিছু ভাইরাস উপেক্ষা করতে পারে না। এ ঘটনা ভাইরাসের উপস্থিতি নিশ্চিৎ করে।

ফাইল ভিত্তিক উপসর্গ সমূহ :

* **ফাইল সংখ্যা বৃদ্ধি পাওয়া :** হঠাৎ করে কোন ডিস্কে স্বাভাবিকের তুলনায় ফাইল সংখ্যা বেড়ে গেলে তা অবশ্যই একটা লক্ষণীয় ব্যাপার। এরূপ ক্ষেত্রে ডাইরেক্টরীতে কোন অপরিচিত ফাইলের নাম থাকলে তা ভাইরাস ফাইল হয়ে থাকতে পারে। এছাড়া কখনও কখনও গুপ্ত (Hidden) ফাইলের সংখ্যাও বেড়ে যাবে যা ডস CHKDSK কম্যাণ্ড বা কোন ডস ইউটিলিটি প্রোগ্রাম দিয়ে দেখে নিয়ে অপরিচিত ফাইল সম্পর্কে নিশ্চিৎ হওয়া যায়।

* **ফাইলের মধ্যে পরিবর্তন ঘটা :** ডিস্কে রক্ষিত সিষ্টেম ফাইলগুলো সাধারণতঃ সিষ্টেম তৈরীকারী প্রতিষ্ঠান কর্তৃক তৈরী এবং সংশোধণী হয়ে থাকে। ফলে এতে যে তারিখ ও সময় নির্দেশক থাকে (যা ডাইরেক্টরী লিষ্ট করলে দেখা যায়) সেটা পুরানো হয়ে থাকে। কিন্তু কখনও যদি এরূপ কোন ফাইলের তারিখ ও সময় পরিবর্তিত হয়েছে বলে মনে হয় তাহলে বুঝতে হবে ফাইলটিতে কিছু সংশোধনী বা বর্ধিত হয়েছে। এটি যদি আপনার দ্বারা পরিবর্তিত না হয়ে থাকে তাহলে নিশ্চিৎ ভাবে ধরে নেয়া যেতে পার ডিস্কটি কোন ফাইল ভাইরাস কর্তৃক আক্রান্ত। কিছুক্ষণ সিস্টেমটি চালানোর পর যদি পর পর কয়েকটা ফাইলে একই ঘটনা ঘটে তাহলে ভাইরাসের উপস্থিতি একেবারেই নিশ্চিৎ।

স্ক্রীণ ভিত্তিক উপসর্গ :

* **মেসেজ :** কিছু কিছু ভাইরাস আছে যারা কিছু নির্দিষ্ট মেসেজ স্ক্রীণে দেখায়। এ মেসেজ দেখে ঐ ভাইরাসটির আক্রমণ নিশ্চিৎ হওয়া যায় যেমন – স্টোন্ড (Stoned) ভাইরাস। এটি মাঝে মাঝে স্ক্রীণে দেখায় "Your PC is now Stoned !" আরও অনেক ভাইরাস রয়েছে যারা এরূপ আচরণ করে।

* **স্ক্রীণে কোন বস্তু ছবি প্রদর্শন :** কিছু ভাইরাস আছে যারা স্ক্রীণে কোন সুনির্দিষ্ট মেসেজ দেয়না কিন্তু বিভিন্ন রকমের চিহ্ন বা ছবি স্ক্রীণে দেখায়। এ জাতীয় চিহ্ন বা ছবির মধ্যে রয়েছে বিশেষ ধরণর ক্যারেক্টার প্রদর্শন, হাউসিং বল প্রদর্শন, ক্রীষ্টমাস ট্রি প্রদর্শন, লগো প্রদর্শন ইত্যাদি। এসবের সাথে মাঝে মাঝে কিছু শব্দও উৎপন্ন হয়।

কখনও কখনও প্লেইন স্ক্রীনেও কিছু কিছু উপসর্গ দেখা যেতে পারে। যেমন– কিছু ভাইরাস প্রভাব আছে যা সিজিএ স্ক্রীনের উদ্দেশ্যে লিখা। কিন্তু স্ক্রীন যদি মনোক্রোম হয় তাহলে কমপিউটার হ্যাঙড্ হয়ে যায়। এ ঘটনাটি অবশ্য সব সময় ভাইরাসের উপস্থিতি নিশ্চিৎ করে না।

অন্যান্য উপসর্গ :

ড্যাটা নষ্ট হওয়া — এটি ডিস্ক ভিত্তিকও হতে পারে আবার ফাইল ভিত্তিকও হতে পারে।

ডিস্ক ভিত্তিক : ডাইরেক্টরী এরিয়া (বুট এরিয়া) ছিন্ন ভিন্ন হওয়া বা নষ্ট হওয়া।

- ফ্যাট এরিয়া নষ্ট হওয়া।
- কোন কোন ট্রাক (যেমন-০ ট্রাক) ফর্ম্যাট হওয়া।
- কিছু কিছু গুরুত্বপূর্ণ বা সংকটপূর্ণ (সেক্টর মুছে ফেলা বা ওভাররাইট করা যা ফর্ম্যাট করার সামিল।)
- হার্ড ডিস্কের ক্ষেত্রে পার্টিশন টেবল নষ্ট করা।
- ডিস্কে লষ্ট ক্লাস্টার বা ক্রস লিংকেড ফাইল তৈরী হওয়া যা CHKDSK কম্যাণ্ড দিয়ে সনাক্ত করা যায়।

ফাইলভিত্তিক :

- কোন ফাইলের মধ্যে নতুন কোন ডাটা সংযোজন বা পরিবর্তন ঘটা।
- কোন ফাইল ডিস্ক থেকে মুছে যাওয়া।
- ফাইলের তারিখ বা সময়ে কোন গুরুত্বপূর্ণ পরিবর্তন ঘটা।

সফটওয়্যারের সাহায্যে ভাইরাসের উপস্থিতি নির্ণয় :

সফটওয়্যারের সাহায্যেও একটা ডিস্ক ভাইরাস কর্তৃক আক্রান্ত কিনা তা নির্ণয় করা যায়। এ জাতীয় প্রোগ্রামকে ভাইরাস স্ক্যানিং প্রোগ্রাম বলা হয়। আজকাল অনেক ভাইরাস স্ক্যানীং প্রোগ্রাম বাজারে পাওয়া যাচ্ছে। এদের মাধ্যমে স্ক্যান করে কোন ডিস্কে ভাইরাসের উপস্থিতি সনাক্ত করা যায়। এটি মেমোরীও স্ক্যান করে নেয়। অবশ্য, ইদানিং কালে স্ক্যানার প্রোগ্রামকেও ফাঁকি দিতে পারে এমন সব ভাইরাস লিখা হচ্ছে। বিভিন্ন দেশে ভাইরাস লিখা হচ্ছে যা গুণগত দিক থেকেও বিভিন্ন স্ক্যান বা অ্যান্টি ভাইরাস প্রোগ্রাম যেগুলো লিখা

হয়েছে সেগুলো প্রাপ্ত ভাইরাস গুলোর বৈশিষ্ট্য অনুসারে। ফলে নুতনগুলো স্ক্যানী-এ ধরা নাও পড়তে পারে।

ভাইরাস আক্রমনের প্রতিকারমুলক ব্যবস্থা ঃ

কোন ডিস্কে বা কমপিউটারে ভাইরাসের উপস্থিতি নিশ্চিৎ হওয়ার পর তা ধ্বংস করা বা প্রতিকারের ব্যবস্থা নেয়া আশু প্রয়োজন। এটি বিভিন্নভাবে করা যায়। নিম্নে তা বর্ণিত হল —

*** ভাইরাস বিধ্বংসী প্রোগ্রাম ব্যবহার ঃ**

আজকাল বাজারে অনেক ভাইরাস বিধ্বংসী প্রোগ্রাম পাওয়া যায়। এদের মধ্যেও রকমভেদ রয়েছে। কিছু কিছু রয়েছে যা কোন বিশেষ ভাইরাস ধ্বংস করার জন্য ব্যবহৃত হয় যেমন ঃ DOCTOR-এটি (C) Brain Killer প্রোগ্রাম। আবার কিছু আছে যা দিয়ে কিছু পরিচিত ভাইরাস ধ্বংস করা যায়। যেমন CLEAN - এটি প্রয়োগের নিয়ম হচ্ছে কম্যাণ্ড দিয়ে ড্রাইভের নাম বলে ভাইরাসের নাম লিখে দিতে হয়। যেমন B ড্রাইভ থেকে Stoned ভাইরাস ধ্বংস করতে কমাণ্ড দিতে হবে - A>CLEAN B : [Stoned]। আবার উপরোক্ত প্রোগ্রামগুলো ব্যবহার করতে হয় ভাইরাসের উপস্থিতি ও নাম নিশ্চিৎ হওয়ার পর। কিন্তু আরও কিছু প্রোগ্রাম আছে যেগুলো দিয়ে একসঙ্গে উপস্থিতি পরীক্ষা (scanning) এবং ধ্বংস (Cleanning) একই সঙ্গে করা যায়। যেমন -VBUSTER প্রোগ্রাম। প্রয়োগের নিয়ম VBUSTER <drive-name>। সম্প্রতি অ্যান্টি ভাইরাসের একটা প্যাকেজ প্রোগ্রাম বাজোরে পাওয়া যাচ্ছে। এটি বাজারজাত করেছে যুক্তরাষ্ট্রের CAREMEL Software Engineering নামে একটা প্রতিষ্ঠান। তারা এটির নাম দিয়েছে Turbo Anti Virus সংক্ষেপে TNTVIRUS। এটি এ পর্যন্ত প্রাপ্ত অ্যান্টি ভাইরাস প্রোগ্রামগুলোর মধ্যে মধ্যে সবচেয়ে শক্তিশালী এবং মজার। এটির প্রয়োগের কম্যাণ্ড হচ্ছে TNTVIRUS লিখে এন্টার প্রেস করতে হবে। তাহলে একটা মেনু স্ক্রীনে আসবে। এর প্রয়োগ সম্পূর্ণ রূপে মেনু ড্রাইভেন। অপশন গুলোর মধ্যে উল্লেখযোগ্য হচ্ছে ভাইরাস খোঁজা, খোঁজা এবং ধ্বংস করা, বুট সেক্টর ইম্যুনাইজ করা, সমস্ত সিস্টেম ফাইল সহ বুট সেক্টর ইম্যুনাইজ করা ইত্যাদি।

এডিট করে ভাইরাস প্রোগ্রাম মুছে ফেলাঃ

স্ক্যান করে ভাইরাসের উপস্থিতি ও ধরণ নিশ্চিত হওয়ার পর কোন ডস ইউটিলিটি যেমন PC Tools বা Norton Utilities ইত্যাদি দিয়ে ফাইল ভাইরাস হলে আক্রান্ত ফাইলটিকে বা বুট সেক্টর ভাইরাস হলে বুটসেক্টর এডিটের জন্য ডেকে ভাইরাস ফাইলটিকে বা ফাইল থেকে ভাইরাস প্রোগ্রামের অংশটুকু মুছে ফেলে ডিস্কটিকে আপডেট করে নিলেও ভাইরাস বিতাড়িত হবে। তবে এ প্রক্রিয়া সব ভাইরাসের ক্ষেত্রে সব অবস্থায় কার্যকর নয়। যেমন Stoned -ভাইরাস যদি কোন হার্ডডিস্কের পার্টিশন টেবল আক্রমণ করে তাহলে তা এ প্রক্রিয়ায় বিতাড়িত করা সম্ভব নয়। সেটি সম্ভব CLEAN বা TNTVIRUS প্রোগ্রাম দিয়ে। এ প্রক্রিয়াটি তাদের পক্ষেই প্রয়োগ সম্ভব যারা বিভিন্ন ডস ইউটিলিটির ব্যবহার জানেন এবং প্রোগ্রামের লো-লেভেল কোড বুঝেন।

*** ডিস্ক ফর্ম্যাট করা ঃ** কোন প্রোগ্রাম দিয়ে ভাইরাস ধ্বংস করতে না পারলে অগত্যা ডিস্কটিকে ফর্ম্যাট করে নিলেও ভাইরাস ধ্বংস হয়ে যায়।

ভাইরাস মুক্ত করার সময় কতগুলো বিষয় মনে রাখা ও সতর্কতা দরকার। যেমন —

• বিভিন্ন দেশের বিভিন্ন প্রোগ্রামার আজকাল বিভিন্ন দৃষ্টি ভঙ্গি থেকে ভাইরাস প্রোগ্রাম লিখছে। এদের বেশীর ভাগেরই চেষ্টা হচ্ছে প্রচলিত অ্যান্টিভাইরাসের দৃষ্টি এড়িয়ে যাওয়া যাতে তাদেরকে চিহ্নিত বা ধ্বংস করতে না পারে। প্রচলিত অ্যান্টিভাইরাসগুলো লিখা হয়েছে এ পর্যন্ত প্রাপ্ত ভাইরাসগুলো ষ্টাডি করে। কিন্তু নতুন গুলোর অনেক নতুন এবং অদ্ভুত বৈশিষ্ট্য এ প্রোগ্রামে যুক্ত হয়ে নাও থাকতে পারে। ফলে ভাইরাস ধ্বংসের জন্যে সবসময় পুরোপুরিভাবে কোন অ্যান্টিভাইরাস প্রোগ্রামের ওপর নির্ভরশীল হওয়া যায় না। সেক্ষেত্রে কোন বিকল্প ব্যবস্থা নিতে হবে।

• ভাইরাস মুক্ত করার সময় কোন ফ্রেশ ডস দিয়ে কমপিউটার পুণঃ চালিত করে নিন, অন্যথায় মেমোরীতে অবস্থিত ভাইরাস পুনরায় ডিস্কটিকে আক্রমণ করতে পারে।

• আক্রান্ত ডিস্কের মাষ্টার ব্যাক আপ থাকলে এটিকে ফর্ম্যাট করে নতুন করে মাষ্টার ডিস্ক থেকে কপি করে নিয়ে ব্যবহার করা যেতে পারে।

• ডিস্কটি কোন সিস্টেম ডিস্ক হলে বা এতে নতুন করে কিছু সংযোজন করার প্রয়োজন না হলে রাইট প্রোটেক্টর ট্যাগ লাগিয়ে নিন।

ভবিষ্যৎ সতর্কতা ঃ

ভাইরাসের হাত থেকে ভবিষ্যতে আপনার ডিস্ক ও কমপিউটারকে রক্ষা করতে নিম্নের সতর্কতাগুলো পালন করুণ —

• প্রতি নিয়ত ড্যাটার ব্যাক আপ তৈরী করুন।

• প্রতিটি সিস্টেম ডিস্কের মাষ্টার কপি রাইট প্রোটেক্টর লাগিয়ে সযত্নে রেখে দিয়ে তাদের কপি ডিস্ক দিয়ে কাজ করুন।

• সব সময় ববহৃত সিস্টেম ডিস্কগুলোতে রাইট প্রোটেক্টর ট্যাগ লাগান।

• সব সময় একটা ফ্রেশ ডিস্ক থেকে অপারেটিং সিস্টেম লোড করুন।

• হার্ড ডিস্কসহ মেশিন হলে সেখান থেকেই কোন সিস্টেম লোড করুন।

• অপরিচিত বা বাইরের অন্যের কোন ডিস্ক ব্যবহার করা থেকে বিরত থাকুন, অথবা ব্যবহার একান্ত প্রয়োজনীয় হলে সেটাতে ভাইরাসের অনুপস্থিতি নিশ্চিত হয়ে ব্যবহার করুন।

• অপরিচিত কোন সফ্টওয়্যার ব্যবহার বা মেশিনে নিজের ডিস্ক ব্যবহার থেকে বিরত থাকুন। • প্রমাণিত (Proven) বা সর্বজন স্বীকৃত সফ্টওয়্যার ভিন্ন নতুন কোন সফ্টওয়্যার ব্যবহারের ক্ষেত্রে সতর্ক থাকুন।

• ট্রোজান ভাইরাস কীলার বা প্রোগ্রাম ব্যবহার থেকে সাবধান থাকুন।

• ভবিষ্যতে যাতে আপনার কমপিউটার বা সিস্টেম ডিস্ক ভাইরাস কর্তৃক আক্রান্ত হতে না পারে তার জন্যেও ব্যবস্থা রয়েছে। এ কাজটিকে বলা হয় ইম্যুনাইজেশন (Immunization) বা টিকা দেয়া। এটি দু'রকম হতে পারে। একটি হচ্ছে বুট সেক্টর ইম্যুনাইজেশন - বুট সেক্টর ভাইরাসের আক্রমণ থেকে রক্ষার জন্যে, অপরটি হল সিস্টেম ফাইল ইম্যুনাইজেশন-ফাইল ভাইরাসের আক্রমণ থেকে রক্ষার জন্য। এছাড়া ডস লোড করার পর মেমোরীকেও ইম্যুনাইজ করে দেয়া যায় যাতে করে কমপিউটার চালু থাকা অবস্থায় কোন ভাইরাস বা ভাইরাস আক্রান্ত কোন ফাইল মেমোরীতে লোড হতে না পারে। এর জন্যে IMMUNE, SCANRES, BOOTSAFE ইত্যাদি নামে প্রোগ্রাম রয়েছে। এটি ব্যবহার করা উচিত AUTOEXEC. BAT ফাইলে। IMMUNE প্রোগ্রাম হলে কম্যাণ্ডের ধরণ হবে IMMUNE (Memory Size)। যেমন - ৬৪০ কেবি র‍্যাম বিশিষ্ট কমপিউটারের বেলায় কম্যাণ্ড হবে IMMUNE 640.

উপসংহার ঃ

ভাইরাস আসলে উন্নত মানের প্রোগ্রামারদের এক অদ্ভুদ সৃষ্টি। প্রতি নিয়ত বিভিন্ন দেশে এগুলো লেখা হচ্ছে। সম্প্রতি পার্শ্ববর্তী দেশ ভারতেও ৩/৪ টা ভাইরাস আবিস্কৃত হয়েছে যা ভারতেই লেখা হয়েছে, অবশ্য তাদের প্রতিকার প্রোগ্রামও লেখা হয়েছে। সমস্যা এলে তবেই মানুষ তার সমাধান খুঁজে। ফলে স্বাভাবিকভাবেই বলা যায় আবিস্কৃত অ্যান্টিভাইরাস প্রোগ্রামগুলো যে সব ভাইরাসকে ঠেকাতে পারবে তা মোটেও সত্য নয়। এখনও অনেক ভাইরাস চিহ্নিত করা যায়নি বা চিহ্নিত করা গেলেও তাদের কার্যকারীতার ধরণ নিশ্চিত হওয়া যায়নি। সর্বোপরি এখানে যে সব ভাইরাস নিয়ে আলোচনা করা হল এছাড়াও অনেক ভাইরাসের নাম শোনা যাচ্ছে। এদের বেশীর ভাগই এখনও স্থানীয়ভাবে বিস্তৃত। সারা বিশ্বব্যাপী বিস্তৃতি লাভ করেনি। আমাদের দেশে মাত্র ৪/৫ টি ভাইরাসের আক্রমণ শোনা গেছে। ভাইরাসগুলো বিস্তৃতি লাভ করে আন-অথোরাইজড সফ্টওয়্যার কপির মাধ্যমে, যা আমাদের দেশে অহরহ ঘঠছে। সেদিক থেকে এখানে ভাইরাসের আগমন ঘটা খুব স্বাভাবিক। এ অবস্থায় আমাদের জন্য সতর্কতা অবলম্বন করাটাই প্রধান কাজ হবে বলে আমি মনে করি। একটা অ্যান্টিভাইরাস প্রোগ্রাম সব সময় হাতের কাছে রাখুন এবং আলোচিত সতর্কতা অবলম্বন করে নিরাপদ থাকুন। ♦

সমাপ্ত