কমপিউটার ভাইরাস ঃ পরিচিতি, প্রভাব ও প্রতিকার

নির্মল চন্দ্র চৌধুরী

(গত সংখ্যার পর)

বুট আক্রমণ কারী ভাইরাস সমূহ ঃ

১। পিং-পং ভাইরাস (Ping-Pong Virus)

- অপর নাম-ইটালিয়া ভাইরাস
- আকার – ২ কেবি
- ফ্লপি ও হার্ড ডিস্কের বুট সেক্টর আক্রমণ করে।
- আক্রান্ত ডিস্ক পরার সময় ভাইরাসটি মেমোরীতে লোড হয়ে মেমোরীর নীম্নাংশে অবস্থান নেয় এবং ২ কিলোবাইট জায়গা দখল করে।
- কিছুক্ষণ পর একটা নৃত্যরত বল স্ক্রীনে আসে এবং যতক্ষণ পর্যন্ত কমপিউটার পুণঃচালনা করা না হয় ততক্ষণ পর্যন্ত বলটি স্ক্রীনে নাচতে থাকে।
- মেমোরীতে অবস্থানকালে অপর যেকোন একটা ভাল ডিস্কে কোন কম্যাণ্ড (যেমন - Dir) প্রয়োগ করলেই ভাইরাসটি ঐ ডিস্কটিতে সংক্রমিত হয়।
- কোন ডস ইউটিলিটি দিয়ে ডিস্কটিকে চেক করালে বা ডিস্ক ম্যাপ নিলে দেখা যায় একটা খারাপ ক্লাস্টার রয়েছে, আসলে এটা বুট সেক্টর বা ভাইরাস কর্তৃক দখলকৃত হয়েছে।

২। মিস-স্পেলার ভাইরাস (MisSpeller Virus) :

- এটি টাইপো ভাইরাস নামেও পরিচিত।
- এটি ইজরাইলী পিং-পং ভাইরাসের একটা স্থানান্তর। এর আক্রমনের ধরণও পিং-পং এর মত।
- মেমোরীতে নিম্নাংশে অবস্থান নেয় এবং২ কিলোবাইট জায়গা দখল করে।
- মেমোরীতে অবস্থান নেয়ার পর প্যারালাল পোর্ট দিয়ে যেসব তথ্য আদান প্রদান হয় তাদের মিলিয়ে ফেলে।
- ইংরেজী, হাক্স এবং গাণিতিক ডিজিটগুলো এমন ভাবে মিলিয়ে ফেলে যে, তা মারাত্মক সন্দেহের সৃষ্টি করে। যেমন -V-কে মিশায় W-এর সাথে, C-কে মিশায় S-এর সাথে, J-কে মিশায় G-এর সাথে ইত্যাদি।

৩। ডিস্ক কিলার ভাইরাস (Disk Killer Virus) :

- অপর নাম -ওগর (Ogre) ভাইরাস।
- ডস বুট সেক্টর আক্রমন করে এবং মেমোরীর প্রান্তে অবস্থান নেয়।
- আকার ৮ কিলোবাইট।
- এটি ডিস্কে ৩টি ক্লাস্টার দখল করে এবং ফ্যাট এরিয়াতে ক্লাস্টার গুলোকে খারাপ হিসেবে চিহ্নিত করে।
- কখনও কখনও ফাইলকে আক্রমন করে এবং তখন ফাইলটিকে মুছে ফেলে তার ওপর অবস্থান নেয়।

৪। স্টোন্ড ভাইরাস (Stoned Virus) :

- আকার- ২ কিলোবাইট।
- প্রথম সনাক্ত করা হয় ১৮৮৯ সালের সেপ্টেম্বরে ইজরাইলে।
- অপর নাম — ম্যারিজুয়ানা এবং নিউজিল্যাণ্ড ভাইরাস।
- বুট সেক্টর ভাইরাসগুলোর মধ্যে এটি খুব পরিচিত এবং ক্ষতিকর।
- যখন কোন আক্রান্ত ডিস্ক থেকে মেমোরীতে অবস্থান নেয় তখন এটা স্ক্রীণে দেখায় Your PC is now Stoned-LEAGALIGE MARIJAUANA.
- স্বয়ংক্রিয় ভাবে মেমোরীতে লোড হয় এবং মেমোরীর শেষ অংশে অবস্থান নিয়ে মেমোরীর পরিমানে কমতি ঘটায়।
- ভাইরাসটির মুল বুটসেক্টরকে ফ্লপি ডিস্কের ১নং সাইডের ৩ নং সেক্টরের 0 ট্র্যাকে সংরক্ষিত করে এবং হার্ডডিস্কের 0 সাইডের ৭ নং সেক্টরের 0 ট্র্যাকে সংরক্ষিত করে।
- ডিস্কের ফ্যাট এবং ডাইরেক্টরীর এরূপ মারাত্মক ক্ষতির কারণে আক্রমণকারী সেক্টরে পূর্বে কোন তথ্য থেকে থাকলে তা চিরতরে নষ্ট হয়ে যায়।
- আক্রান্ত হার্ডডিস্ক ব্যবহার করলে ডিস্কে অনেক ব্যাড ক্লাস্টার তৈরী করে যা পরবর্তীতে কোন তথ্য পড়ানোর সময় Read Error মেসেজ দেয়।
- হার্ডডিস্কে আক্রমণ করলে বেশীর ভাগ ক্ষেত্রে তার পার্টিশন টেবল এলাকায় অবস্থান নেয় এবং ডিস্ক পুনঃ ফর্ম্যাট করলেও ভাইরাসটি দুরীভূত হয় না।
- এর ৫টি ধরণ রয়েছে।

৫। ব্রেইন ভাইরাস (Brain Virus) :

- প্রাপ্তিস্থান – ওয়াশিংটন বিশ্ববিদ্যালয়, ভার্শন ভেদে ইজরাইল।
- আকার – ৩ কিলোবাইট
- ভাইরাসের মধ্যে প্রাপ্ত তথ্য থেকে অনুমান করা হয় এটি পাকিস্তানের লাহোর শহর থেকে লেখা হয়েছে।
- ডিস্কের বুট সেক্টর আক্রমণ করে এবং বুট সেক্টরের পূর্বতন তথ্য মুছে ফেলে ঐ স্থানে ভাইরাস প্রোগ্রাম নিজে অবস্থান নেয়।
- ডিস্কের ভলুম লেবেল পরিবর্তন করে '(C) Brain' লিখে, যা দেখে এ ভাইরাসের আক্রমণ নিশ্চিৎ হওয়া যায়।
- আক্রান্ত ডিস্ক থেকে যে কোন সিস্টেম লোড করতে গেলে আগে ভাইরাসটি লোড হয়। এরপর অন্য কোন অনাক্রান্ত ডিস্ক পড়ালে সে ডিস্কেও সংক্রামিত হয়।
- ভাইরাসটি ডিস্কের যে স্থানে অবস্থান নেয় সেখানে ৩ কিলোবাইট জায়গা ব্যাড সেক্টর হিসেবে চিহ্নিত হয়।
- ভাইরাসটি বুট সেক্টরে এমন কৌশলে অবস্থান করে যে সেখানে নতুন কিছু লিখে (যেমন নতুন করে লেবেল নামকরণ করলে) ওকে তাড়ানো যায় না। নতুন কিছু লিখতে গেলে প্রতিবারই ভাইরাসটি মূল বুট সেক্টর দখল করে নেয়।

৬। বুট কিলার ভাইরাস (Boot Killer Virus) :

- বুট সেক্টর আক্রমণ করে একেবারে নষ্ট করে ফেলে, সেজন্যে এরূপ নামকরণ।
- হার্ড ডিস্ক আক্রান্ত হলে প্রতিদিন গড়ে ২ মেগাবাইট লস্ট ক্লাস্টার চেইন তৈরী করে এবং ডসের CHKDSK/I কম্যাণ্ড ছাড়া এটি বুঝা যায় না। পরে CHK এক্সটেনশনের ফাইলগুলো মুছে ফেলে পুনরুদ্ধার সম্ভব।
- সবচাইতে ক্ষতিকর দিক হচ্ছে, কখনও কখনও এটি ডিস্কের প্রথম ট্র্যাকটি (0 ট্র্যাক) ফর্ম্যাট করে। কিন্তু ফর্ম্যাট করে সাধারণ ৯টি সেক্টরের ৮টি। ফর্ম্যাটের পরে এ সেক্টরগুলোর নম্বর করণ করে ২ থেকে ৯ পর্যন্ত। এর ফলে কমপিউটার ডিস্কটিকে পড়তে গিয়ে ডসের নিয়ম অনুসারে ১ নং সেক্টর খুঁজে পায়না, যেটি বুট সেক্টর হওয়া উচিৎ এরূপ ক্ষেত্রে স্বাভাবিকভাবেই ডিস্কের সমস্ত তথ্য নষ্ট হয়ে যায় এবং ডিস্কটিকে নতুন করে ফর্ম্যাট করে নিয়ে কাজ করতে হয়।

(চলবে)