পিসি ভাইরাস আক্রান্ত কী করব?

তাসনুভা মাহ্‌মুদ

কমপিউটার জগৎ-এর নিয়মিত বিভাগ পাঠশালা সাধারণত ব্যবহারকারীদের ব্যবহারগত প্রয়োজনীয়তা ও চাহিদার প্রতি লক্ষ রেখে বিভিন্ন বিষয়ের ওপর লেখা প্রকাশ করে আসছে। তারই ধারাবাহিকতা থেকে একটু ভিন্ন দৃষ্টিকোণে সেপ্টেম্বর ২০১৩-এর পাঠশালায় উপস্থাপন করা হয়েছিল কুখ্যাত ২০ ওয়ার্ম, ভাইরাস ও বটনেক সম্পর্কে প্রাথমিক ধারণা। কেননা গত চার দশকের বেশি সময় ধরে অসংখ্য ম্যালওয়্যারের ব্যাপক বিস্তারের ঘটনা পরিলক্ষিত হয়। আর তাই এবারের পাঠশালা বিভাগে উপস্থাপন করা হয়েছে ম্যালওয়্যার, ওয়ার্ম, ভাইরাস থেকে পরিত্রাণের উপায় নিয়ে। লক্ষণীয়, ব্যবহারকারীদের সর্বোত্তম প্রচেষ্টা থাকা সত্ত্বেও সবচেয়ে খারাপ ব্যাপারগুলো ঘটতে থাকে ম্যালওয়্যার ভাইরাস সংক্রমণের কারণে। এ ধরনের সমস্যা সমাধানের চেষ্টা করার আগে নিজে নিজে কিছু বিষয় জানতে চেষ্টা করুন।

আপনার কমপিউটার কী ধীরগতিতে রান করে, ঘন ঘন ক্র্যাশ করে এবং সাধারণত খুব অস্বাভাবিক আচরণ করে? ধরুন, আপনি একটি ওয়েব ব্রাউজারে ফায়ার করলেন, কিন্তু ওই সাইটে না গিয়ে এমন এক সাইটে চালিত হলেন, যেখানে আপনি ভিজিট করতে চাননি। এমন ঘটনা কি সচরাচর ঘটে থাকে? আপনি যখন ব্রাউজার ব্যবহার না করেন, তখনও কি পপ-আপ আবির্ভূত হয়? যদি আপনি শঠতাপূর্ণ সার্চ ইঞ্জিন অ্যাড-অনস ও অন্যান্য অনাকাঙ্ক্ষিত ব্রাউজার এক্সটেনশনে চেক করেন এবং সিস্টেম টেম্পোরারি ফাইল ও অন্যান্য ব্লট উপাদানকে সিস্টেম থেকে দূর করার জন্য 'crap cleaner' রান করেন এবং এটিকে অন্যদের থেকে আলাদা করেন, তাহলে ধরে নিতে পারেন এখন সময় হয়েছে সংক্রমণ শনাক্ত করা এবং তা অপসারণের জন্য চিন্তা-ভাবনা করা। যদি ব্যাপারটি এমন হয়, তাহলে নিচে বর্ণিত ধাপগুলো অনুসরণ করুন, যেখানে ব্যাখ্যা করে দেখানো হয়েছে, পিসিকে আগের ভালো অবস্থায় রান করানোর জন্য কী করা যায়।

ইন্টারনেট সংযোগ বিচ্ছিন্ন করা

কমপিউটার ম্যালওয়্যার আক্রান্ত হলে আমাদের চারপাশের বিভিন্ন ব্যবহারকারীর কাছ থেকে অনেক উপদেশের কথা শোনা যায়, যেখানে পরামর্শ দেয়া হয়, আপনার প্রথম পদক্ষেপ হলো অনলাইনে গিয়ে স্ক্যানিং প্রোগ্রাম রান করা, যা হতে পারে লাইসেন্স অ্যান্টিভাইরাস প্রোগ্রাম কিংবা ফ্রি অ্যান্টিভাইরাস টুল, যা অপারেটিং সিস্টেম থেকে পেতে পারেন বা অ্যান্টিভাইরাস ভেন্ডরের কাছ থেকে ফ্রি ডাউনলোড করে নিতে পারেন। ভাইরাস স্ক্যানিংয়ের ব্যাপারটি এখন খুব সাধারণ বিষয়, তাই কার্যকরভাবে ভাইরাস অপসারণের জন্য আমাদেরকে প্রথমে জানতে হবে কী আক্রান্ত হয়েছে। বাস্তবতা হলো, যেখানেই ইন্টারনেট সংযোগ সক্রিয় সেখান থেকেই ম্যালওয়্যার কার্যকরভাবে বিকশিত হতে পারে, যাকে বলা যায় সম্ভাব্য লাইভ ইনফেকশনের সূত্রপাত হওয়া।

আমাদের অনেকেরই জানা নেই, কখনও কখনও খুব পরিচিত সেরা সিকিউরিটি ভেন্ডর সাইটকেও ম্যালওয়্যার যেমন ব্লক করে দিতে পারে, তেমনি ম্যালওয়্যারগুলো অফার করতে পারে কিছু টুল, যেগুলো দিয়ে স্ক্যান ও সংক্রমণকে দূরীভূত করা যায়। এজন্য অনলাইনে যুক্ত হতে হয়, যা সময় অপচয় করে। যখনই বুঝতে পারবেন কোনো সাইটে সমস্যা রয়েছে, তাহলে সতর্কতামূলক ব্যবস্থা হিসেবে যত দ্রুত সম্ভব রাউটারের প্লাগ খুলে ফেলুন, যাতে ইন্টারনেট সংযোগের মাধ্যমে ডাটা কম্প্রোমাইজকে থামানো যায়।

ম্যালওয়্যার স্ক্যানার ডাউনলোড করা

যদি আপনার সিস্টেমে একটি অ্যান্টিভাইরাস স্ক্যানার রানিং থাকে, তারপরও ম্যালওয়্যার আপনার সিস্টেমে রান করতে থাকবে। মনে হবে ওই সফটওয়্যার কম্প্রোমাইজ হয়ে গেছে। ম্যালওয়্যার সম্ভবত আপনার সিস্টেমের আপডেট প্রক্রিয়াকে ডিজ্যাবল করে দিয়েছে,

অর্থাৎ ম্যালওয়্যার আপনার সিস্টেমে আন্টিভাইরাস আপডেটকে যথাযথভাবে সিস্টেমে লোড হতে দিচ্ছে না। অবস্থা যাই হোক, ম্যালওয়্যার শনাক্তকরণ ও অপসারণ প্রসেসের সময় স্ক্যানারকে অন্ধের মতো বিশ্বাস করাটা হবে বোকামি। বিশ্বের বিভিন্ন ল্যাব টেস্টের রিপোর্ট ও জগৎখ্যাত বিভিন্ন আইসিটিবিষয়ক পত্রিকায় প্রকাশিত বিভিন্ন রিপোর্ট থেকে জানা যায়, কোনো সিকিউরটি স্যুট অথবা অ্যান্টিভাইরাস স্ক্যানারই শতভাগ যথাযথ নয় এবং কোনো টুলই সব ম্যালওয়্যার হুমকিকে শনাক্ত করতে পারে না।

দুই বা ততোধিক ফ্রি অ্যান্টিভাইরাসের সমন্বয়ে তুলনামূলকভাবে ভালো ফল পাওয়া যাবে। প্রথমে একটি টুল রান করুন এবং যেকোনো রিমোভাল রিকোমেন্ডেশন অনুসরণ করুন। এরপর যখন সিস্টেম রিবুট হবে, তখন একই কাজ করুন পরবর্তী অ্যান্টিভাইরাস টুল ব্যবহার করে। একই প্রসেস অনুসরণ করে সর্বশেষ অ্যান্টিভাইরাস টুল।

এ প্রসেস সম্পন্ন করার পর যদি তিনটি সিস্টেমই আপনার সিস্টেমকে একটি পরিষ্কার সিস্টেম হিসেবে প্রদর্শন করে, তাহলে নিশ্চিত থাকতে পারেন আপনার সিস্টেমটি খুবই নিরাপদ ও ইউজার ফ্রেন্ডলি।

আপনার হাতের কাছে যদি প্রয়োজনীয় টুল না থাকে, তাহলে অন্য কমপিউটার থেকে একটি পরিষ্কার নতুন ফরম্যাট করা ইউজার ড্রাইভে এক্সিকিউটেবল ফাইল ডাউনলোড করে নিন, যা থাকবে সংক্রমণ মুক্ত। তবে সম্পূর্ণ স্ক্যানিং প্রসেস দ্রুততর হবে এমনটি আশা করা ঠিক হবে না। অর্থাৎ স্ক্যানিং প্রসেস দ্রুততর না করে স্বাভাবিকভাবে সম্পন্ন করুন। এজন্য ফুল ডিপ স্ক্যান অপশন যাতে টিক থাকে তা নিশ্চিত করুন। এটি বেশ সময় সাপেক্ষ একটি প্রসেস, যা সম্পন্ন হতে কয়েক ঘণ্টা লাগতে পারে। এ ক্ষেত্রে আপনি ব্যবহার করতে পারেন ক্যাসপারস্কি টিডিএসএসকিলার (Kaspersky TDSSKiller) টুল, যা একটি ফ্রি ম্যালিশাস রুটকিট। এটি ক্ষতিকর ইউটিলিটি শনাক্ত ও অপসারণ করে। অনেক সময় রুটকিট বিশেষভাবে বিরক্তির কারণ হয়ে দাঁড়াতে পারে, কেননা এগুলো বলপূর্বকভাবে-গভীরভাবে লো লেভেলে উইন্ডোজ এপিআইয়ের অন্তর্নিহিত অর্থোপলব্ধি করতে চেষ্টা করে।

ফোল্ডার ফাইল, প্রসেস ও রেজিস্ট্রি কী ইত্যাদি লুকিয়ে রাখার মাধ্যমে একটি রুটকিট নিশ্চিত করতে পারে অ্যান্টিভাইরাসের স্ক্যানারের মতো ম্যালওয়্যার ইউজারদের কাছে অদৃশ্যভাবে থেকে যেতে পারে। রুটকিট খুব দ্রুতগতিতে স্ক্যান করতে পারে, যা বেশিরভাগ ম্যালওয়্যার স্ক্যানের ক্ষেত্রে দেখা যায় না। রুটকিট স্ক্যান ▸

করতে মাত্র এক মিনিট বা কয়েক মিনিট সময় নেয়। টিডিএসএসকিলার রিমোভাল প্রসেসকে এমন সহজতর করেছে যে শুধু এক বাটন চাপলেই হয় এবং কাজ শেষে পিসি রিবুট করতে হয়।

সেফ মোডে স্টার্ট করা

অবশ্যই একটি ডেডিকেটেড ম্যালওয়্যার স্ক্যানার ব্যবহার করা উচিত। তবে সেফ মোডের বাইরে থেকে এ কাজটি কোনোভাবেই করা উচিত নয়। সেফ মোডের ভেতরে থেকে ম্যালওয়্যার স্ক্যানার চালু করা উচিত সবসময়। কেননা উইন্ডোজ ওএসের ন্যূনতম ভার্সন মূলত জেনেরিক ড্রাইভার ছাড়া আর কিছুই ব্যবহার করে না। এটি অবশ্যই স্টার্টআপ অ্যাপের তত্ত্বাবধান করে না, যার ওপর বেশিরভাগ ম্যালওয়্যার নির্ভর করে। কোনো টুলই শতভাগ নিশ্চয়তা দিতে পারে না, কেননা কিছু অ্যাডভান্স ম্যালওয়্যার এ সীমাবদ্ধতাকে এড়িয়ে যেতে সক্ষম হবে।

আমরা মোটামুটিভাবে সবাই জানি, সেফ মোড সাধারণত চালু হয় বুটিং প্রসেস চলাকালে তাৎক্ষণিকভাবে F8 কী চাপলে, যদি না আপনি উইন্ডোজ ৮ ব্যবহার না করেন। কেননা মাইক্রোসফট পিসির বুটিং গতি বাড়ানোর জন্য এ অপশনকে সরিয়ে ফেলেছে।

উইন্ডোজ ৮ ব্যবহারকারীরা সেফ মোডে অ্যাক্সেস করতে পারবেন উইন্ডোজ +R কী একত্রে চেপে। এরপর এমএস কনফিগ টাইপ করে এন্টার চাপুন। এবার বুট ট্যাব সিলেক্ট করে বুট অপশন সেটিংয়ের অন্তর্গত সেফ মোড চেকবক্সে ক্লিক করুন। এতে পিসি রিস্টার্ট করার পর আপনি সেফ মোডে প্রবেশ করতে পারবেন। উইন্ডোজ ৮ কল করে নরমাল Safe Mode Minimat। কমান্ড প্রম্পটসহ সেফ মোড স্টার্ট করাকে বলে alternate shell এবং নেটওয়ার্কসহ স্টার্ট করাকে বলে Network।

সফলভাবে ম্যালওয়্যার সংক্রমণ দূর করার পর স্বাভাবিক বুটিং প্রসেসে ফিরে যেতে চাইলে এমএস কনফিগ প্রসেসকে পুনরাবৃত্তি করতে হবে। বাস্তব জীবনে ব্যবহারকারীরা রানসামওয়্যার (ransomware) দিয়ে আক্রান্ত। এরা লিনআক্স পরিবেশে বুট ও নেভিগেট করতেও ব্যর্থ হয়।

এখন প্রশ্ন হচ্ছে, যদি সেফ মোডে ঢুকতে না পারেন, তাহলে কেমন হবে? কিছু ম্যালওয়্যার যেমন সাম্প্রতিককালের এফবিআই রানসামওয়্যার আপনার কমপিউটারকে লক ডাউন করবে, যাতে কমান্ড প্রম্পট দিয়ে সেফ মোডে অ্যাক্সেস করতে না পারেন। এর ফলে রিমোভাল প্রসেস বাধাগ্রস্ত হবে। তবে যাই হোক, ভাইরাস আক্রান্ত ফাইলকে অপসারণ করার আরও উপায় রয়েছে।

এমন অবস্থায় অভিজ্ঞ ব্যবহারকারীরা উপদেশ দেন পিসিকে লিনআক্স পরিবেশে সিডি বা ইউএসবি ড্রাইভ থেকে রিবুট করতে। এর ফলে আপনি আক্রান্ত ফাইল ম্যানুয়ালি শনাক্ত ও অপসারণ করতে পারবেন। দুর্ভাগ্যজনকভাবে এ প্রক্রিয়াটি শুধু অভিজ্ঞ ব্যবহারকারীদের জন্য।

আপনি ইচ্ছে করলে থার্ড পার্টি টুল ব্যবহার করতে পারেন। এ ক্ষেত্রে HitmanPro.kickstart নামে ম্যালওয়্যার রিকোভারি টুল কিট ব্যবহার করতে পারেন। এটি একটি ফ্রি টুল ৩০ দিনের জন্য। হিটম্যানপ্রোর অংশ হিসেবে দ্বিতীয় অপশন হলো second opton ম্যালওয়্যার স্ক্যানার। আপনাকে এ ইউটিলিটি ডাইনলোড করে ইউএসবি ড্রাইভে নিতে হবে। এরপর এটি দিয়ে কমপিউটার বুট করুন। এখানে এ টুল পরিচালনা করার জন্য ভিডিও গাইড ও ধাপে ধাপে ইনস্ট্রাকশন পাবেন।

সুপরিচিত উইন্ডোজ পরিবেশে থেকে হিটম্যানপ্রো ডট কিকস্টার্ট শুধু যে সহজে ব্যবহারকারীর জন্য পরিষ্কার পরিচ্ছন্ন সিস্টেম রান করে তা নয়, বরং সফটওয়্যারও পরিপাটি করে এটি। যেহেতু এটি ব্যবহার করে 'live', রানস্যাম উইন্ডোজ পরিবেশ, তাই এর রয়েছে চালু হওয়া সব ধরনের ফরেনসিক তথ্য প্রসেসে অ্যাক্সেস সুবিধা। যেমন ডেস্কটপ ও অন্য সবকিছু ব্লক করার জন্য যে প্রসেস ফুল স্ক্রিনে রান করে ইত্যাদি। এর অর্থ হচ্ছে এটি নির্দিষ্ট করতে পারে কোনো ফাইল ও রেজিস্ট্রি কী ম্যালওয়্যার সৃষ্ট। ফলে একটি স্বয়ংক্রিয় রিমোভাল প্রসেসে সক্রিয় থাকে।

ম্যালওয়্যার অপসারণ করার কাজ সম্পন্ন করার পর আবার স্ক্যান করুন deep মোডে। এটি সময় সাপেক্ষ ব্যাপার হলেও আপনার সিস্টেমের বিভিন্ন লোকেশনে ম্যালওয়্যার আবার ইনস্টল হয়নি তা নিশ্চিত করার জন্য এ প্রসেসের শেষ ধাপ সম্পন্ন করা উচিত। কিছু কিছু ম্যালওয়্যার আছে যেগুলোকে কোনোভাবে অপসারণ করা যায় না। যদি আবার স্ক্যানে সংক্রমণ দেখা যায়, সে ক্ষেত্রে থেকে যাওয়া একমাত্র নিরাপদ অপশন হলো nuke and pave, যেখানে ডিস্ক ফরম্যাট ও উইন্ডোজের রিইনস্টলেশন সম্পন্ন হয়, এর সাথে সমন্বিত থাকে রিয়েল টাইম প্রটেকশন। এরপরও যদি পিসি সংক্রমণের সঙ্কেত দেখায়, তাহলে আপনাকে পরবর্তী ধাপের জন্য মুভ করতে হবে, যা খুবই কঠিন কাজ, যার জন্য দরকার অভিজ্ঞদের সহায়তা ও পরামর্শ।

সহায়তা নেয়া

ইদানীংকার ম্যালওয়্যার প্রায় সময় অপারেটিং সিস্টেমে রেখে যায় জটিল ওয়েব হুক। তবে সৌভাগ্যের কথা, এজন্য প্রচুর সহায়তা পাওয়া যায়। তবে সুনিশ্চিত না হয়ে সর্বোত্তম সহায়তা পাওয়ার আশায় না জেনে কোনো কিছুতে ক্লিক করার অর্থ ভয়াবহ বিপদের মুখে পড়ার সম্ভবনা। তাই না জেনে কোনো কিছুতে ক্লিক করা উচিত হবে না। আপনার ভাইরাস আক্রান্ত পিসিতে যে ম্যালওয়্যার রয়েছে তার নাম যদি জানেন, তাহলে অনলাইনে গিয়ে একটি পরিষ্কার কমপিউটার ব্যবহার করে অ্যান্টিভাইরাস ভেন্ডর ওয়েবসাইটে ভিজিট করুন ওই হুমকি সংশ্লিষ্ট উপদেশের জন্য, যা প্রয়োগে ভাইরাস অপসারণ করা যায়। যদি কাঙ্ক্ষিত সহায়তা খুঁজে পাওয়া না যায়, তাহলে সিস্টেমের সিকিউরিটির জন্য ডেডিকেটেড ফোরামের সাথে যোগাযোগ করতে পারেন।

ম্যালওয়্যার থেকে কার্যকরভাবে পরিত্রাণের উপায় জানিয়ে সহায়তা দেয়ার উদ্দেশ্যে বেশ কিছু ফোরাম রয়েছে, যারা ব্যবহারকারীদেরকে বিশেষজ্ঞের পরামর্শ দিয়ে থাকে, যেগুলো সুনির্দিষ্ট হুমকিসংশ্লিষ্ট। এ ফোরামগুলোর মধ্যে অন্যতম হলো ডিএসএসএল সিকিউরিটি ফোরাম, ব্লিপিং কমপিউটার ও ড্যানির ওয়েব, ভাইরাসেস, স্পাইওয়্যার অ্যান্ড আদার ন্যাস্টিস ইত্যাদি।

প্রতিটি ফোরামের নিয়মকানুন অনুসরণ করার জন্য নিজেকে প্রস্তুত করুন। এমন অবস্থায় যদি প্রথমেই একটি ফ্রি ডায়াগনস্টিক টুল ডাউনলোড করতে বলা হয় ফোরাম থেকে, তাহলে বিস্মিত হবেন না। ডায়াগনস্টিক টুল ডাউনলোড করে কয়েকবার স্ক্যান রান করুন। এর ফলে একটি লগ ফাইল তৈরি হবে, যার মাধ্যমে বিশেষজ্ঞেরা ম্যালওয়্যার ক্লিনআপ প্রক্রিয়ার জন্য প্রয়োজনীয় উপদেশ দিতে পারবে।

সিস্টেম রিস্টোর এড়িয়ে যাওয়া

যদি আপনি ম্যালওয়্যারের শিকার হন, তাহলে সিস্টেম রিস্টোর ব্যবহার করার পরিবর্তে তা ডিজ্যাবল করুন। অবশ্যই এটি কোনো ভালো উপদেশ হিসেবে বলা যায় না, কেননা সিস্টেম রিস্টোর টুল আপনার ক্ষতিগ্রস্ত সিস্টেমকে সর্বশেষ আগে ভালো অবস্থায় পিসিকে ফিরিয়ে আনতে সহায়তা করে, যাতে পিসি স্বাভাবিকভাবে কাজ করতে পারে।

কখন কমপিউটার সংক্রমিত হবে তা এ লজিকের মাধ্যমে জানা যায় না, যা এ লজিকের একটি ত্রুটি। তবে সিস্টেম রিস্টোর খুব সহজে ও সফলতার সাথে ব্যাকআপ করবে এবং ইনফেকশনকে আপনার জন্য রিস্টোর করবে। তবে এটি ভালো হতে পারত যদি আপনার ম্যালওয়্যার সহায়কভাবে ফাংশনে অ্যাক্সেসকে কোনোভাবে ডিজ্যাবল করতে পারত। যদি না হয়, তাহলে কন্ট্রোল প্যানেলে গিয়ে এটি ডিজ্যাবল করুন। এজন্য ক্লিনআপ প্রসেসের পর System→Performance→Troublshoting ইউনিটে অ্যাক্সেস করুন। এবার কমপিউটার আবার স্টার্টআপ করার জন্য আগে ভালো ফলাফলের জন্য সব রিস্টোর পয়েন্ট ডিলিট করুন কজ

ফিডব্যাক : mahmood_sw@yahoo.com